BRANDEFENSE COUNTRY REPORT · SWITZERLAND 2026

Brandefense Suisse : rapport sur le paysage des cybermenaces 2026

Abus d'identité, incidents chez les fournisseurs et reprise des services interconnectés

Odin by Brandefense
Période de recherche: 1 janvier–22 novembre 2026, selon la date des publications
Version 1.0 · Édition publique de recherche · TLP:CLEAR · 22 novembre 2026

49 des 250
organisations avaient un identifiant proposé à la vente lors de la vérification

5
études de cas distinguant données annoncées et incidents vérifiés

97 000
enregistrements de permis, sans compter les personnes

41
noms de groupes dans l'instantané suisse des rançongiciels

TABLE DES MATIÈRES

Table des matières

Translated with AI

Cette édition a été traduite avec l'aide de l'intelligence artificielle à partir de l'original anglais; la version anglaise fait foi.

01	Synthèse	04
	Carte du rapport	08
	Sommaire et parcours de lecture	09
02	Contexte numérique et paysage des menaces en Suisse	10
03	Exposition nationale : la population d'organisations sélectionnée	16
04	Offres du dark web et limites des éléments disponibles	24
05	Exemples de ciblage par secteur	40
06	Hacktivisme et DDoS	56
07	Acteurs de la menace et relations étayées	61
08	Économie de la fraude : identité, confiance et paiement	72
09	Analyse approfondie de la banque	77
10	Réglementation et réponse nationale	81
11	Perspectives	86
12	Plan d'action	91
	Annexes	96
A	Annexe A. Périmètre, sources et confiance	97
B	Annexe B. Registre des éléments	99
C	Annexe C. Sources	101
D	Annexe D. Glossaire	106
	À propos du rapport	108

Conseil d'administration et RSSI	01 05 11 12
SOC et réponse aux incidents	04 06 07 12
Identité et infrastructure	03 05 07 12
Fraude et banque	08 09 12
Juridique et achats	05 10 12

À propos de cette édition

Traduit avec l'IA. En cas de divergence, la version anglaise fait foi.

Recherche et rédaction assistées par l'IA. Les affirmations criminelles, les communications officielles et les interprétations des analystes restent distinctes. L'annexe A précise le périmètre et les niveaux de confiance.

Les éléments disponibles en Suisse justifient des investissements conjoints dans les contrôles d'identité, les notifications des fournisseurs et les tests de reprise. Les annonces clandestines restent distinctes des incidents confirmés.

122

inscriptions suisses sur des sites de rançongiciels pendant la période étudiée

250

organisations candidates sélectionnées dans treize secteurs

48 / 100

indicateur national Atlas pour 247 organisations candidates évaluées ; des valeurs plus élevées indiquent une exposition observée plus forte

4

décisions avec responsables désignés et preuves de réalisation

CHAPITRE 01

Synthèse

01

CE CHAPITRE RÉPOND À LA QUESTION

Quelles décisions de sécurité les éléments suisses justifient-ils ?

4

décisions avec responsables et preuves de réalisation

Quatre décisions pour la direction 06

L'année en chiffres 06

CHAPITRE 01

Synthèse

EN BREF

Les éléments suisses relient abus d'identité, incidents fournisseurs et risque de reprise. Ransompedia recense 122 inscriptions suisses pendant la période étudiée. Des identifiants associés à 49 des 250 organisations sélectionnées étaient proposés à la vente lors de la vérification. L'indicateur national Atlas atteint 48 sur 100 pour 247 organisations évaluées. Les avis officiels préservent les incertitudes sur services et données. Priorisez validation des comptes, notifications fournisseurs, restauration indépendante et communications fondées sur des faits établis.

Ce rapport associe les publications Brandefense Blackhole, les inscriptions Ransompedia, les observations d'exposition Atlas et les contrôles passifs aux informations publiques vérifiées. Chaque population répond à une question différente. Ni publications ni inscriptions ne comptent des intrusions vérifiées. Les organisations sélectionnées ne représentent pas la prévalence nationale [S1][S2][S3].

1. Les inscriptions d'extorsion justifient une planification de continuité dans plusieurs secteurs. Le total suisse atteint 122 inscriptions pendant la période 2026 indiquée, contre 50 sur l'ensemble de 2025. Ces périodes inégales ne permettent pas de mesurer un taux d'attaque. AKIRA représente 13 inscriptions, The Gentlemen et Qilin 9 chacune. Le reste se répartit entre de nombreux autres noms de groupes. Une inscription ne prouve pas indépendamment le chiffrement, le vol de données ou un paiement [S2].

L'instantané régional recense 457 inscriptions pour l'Allemagne, 295 pour la France, 286 pour l'Italie et 61 pour l'Autriche. Ces populations de tailles différentes présentent aussi des couvertures différentes d'observation et de divulgation. Elles contextualisent la planification de reprise, sans classer la sécurité des pays [S2].

Les pays de comparaison ont été choisis à titre d'exemples uniquement pour apporter du contexte ; leur sélection n'implique ni classement ni appréciation politique.

2. Les communications officielles placent les abus d'identité aux côtés des rançongiciels. L'Office fédéral de la cybersécurité recense 27 128 signalements volontaires et 200 annonces obligatoires au premier semestre 2026, contre 29 006 signalements volontaires et 145 annonces obligatoires au second semestre 2025 [S5][S107]. Son rapport du premier semestre 2025 comptait 35 727 signalements sous un total unique et 57 signalements de rançongiciels, contre 79 cas de rançongiciels signalés et observés au premier semestre 2026 [S5][S108]. Ces populations officielles ont des définitions propres à chaque période et ne doivent pas être ajoutées aux totaux de ce rapport [S5][S107][S108].

L'office souligne le phishing visant les comptes cloud et l'usurpation de cadres ou de services d'assistance. Un message crédible peut convaincre une personne de révéler son mot de passe, d'approuver une connexion ou d'installer un logiciel. Il faut vérifier l'autorité par un canal fiable distinct. En cas d'abus suspecté, examinez ensuite les sessions et les paramètres de récupération [S5].

3. Les incidents chez les fournisseurs exigent des décisions techniques et de notification. Une organisation peut dépendre d'un sous-traitant pour la prévoyance, la santé, les médias, les clients ou le personnel. Ses premières informations fiables peuvent donc venir d'un prestataire. Le responsable du traitement doit toujours identifier ses propres données, processus touchés et obligations d'annonce. Le chapitre 5 conserve les incertitudes de chaque avis officiel concernant les accès et les extractions.

L'enquête d'un prestataire ne devrait pas retarder l'évaluation initiale du risque par son client. Une annonce d'attaquant ne devrait pas non plus devenir la version publique de l'organisation. Conservez l'avis, établissez le service concerné et identifiez les preuves de chaque déclaration sur les données.

4. La récente communication cantonale distingue enregistrements et personnes. L'avis du 20 novembre décrit environ 97 000 enregistrements dans une application administrative. Les permis répétés et les prolongations signifient que ce total n'est pas celui des personnes concernées. Le même avis décrit l'isolement de la plateforme et la poursuite du traitement par des formulaires de remplacement. Ce cas concerne le service et la gestion des données. Il ne permet pas d'élargir le nombre de résidents touchés [S16].

5. Les observations externes d'identité exigent la validation des comptes. Le portefeuille évalué recense au moins 172 240 associations d'appareils et 11 072 599 associations historiques d'identifiants. Des identifiants associés à 49 des 250 organisations sélectionnées étaient proposés à la vente lors de la vérification. Les observations couvrent 247 organisations ; 3 n'ont pas de résultat d'exposition. Aucune population ne compte des intrusions confirmées ou personnes distinctes. Validez comptes actuels, activité pertinente et corrections antérieures avant toute action perturbatrice [S3].

6. Les délais d'annonce exigent un arbre de décision préparé. Les annonces concernant les infrastructures critiques, les données personnelles et la surveillance financière ont des déclencheurs et délais différents. Une liste générique peut manquer ces différences. Les équipes juridiques et de gestion d'incident devraient déterminer les obligations susceptibles de se cumuler avant qu'un événement réel n'impose cette discussion [S6][S7][S8].

Quatre décisions pour la direction

1. **Validez les signaux d'identité à partir de l'activité réelle.** Chargez l'équipe identité de rapprocher les nouvelles offres et alertes de phishing des comptes actifs, sessions et changements de récupération. Conservez les preuves avant de réinitialiser les accès. Transmettez tout usage non autorisé corroboré au processus de gestion d'incident.
1. **Exercez la notification avec les fournisseurs essentiels.** Les achats, responsables de services et juristes devraient simuler une alerte initiale de prestataire. Confirmez les données et processus dépendants, les personnes capables de conserver les traces et celles qui lancent chaque évaluation d'annonce.
1. **Restaurez un service essentiel de manière indépendante.** Confiez aux équipes continuité et infrastructure un test utilisant des sauvegardes protégées et des identifiants de reprise distincts. Exigez une validation métier du service et des données récupérés, en plus du résultat technique.
1. **Séparez le traitement des affirmations des communications publiques sur l'incident.** Désignez un responsable de communication, un responsable des preuves et un canal de secours pour l'état des services. Consignez les affirmations, les impacts observés et ce que l'organisation peut établir sur les données.

L'année en chiffres

Les chiffres décrivent des populations distinctes. Une mesure indisponible n'est pas un zéro.

Nombre	Ce qu'il représente	Ce qu'il ne représente pas
122	Inscriptions suisses de rançongiciels pendant la période étudiée [S2]	Intrusions vérifiées, victimes uniques ou prévalence nationale
50	Inscriptions suisses datées de l'ensemble de 2025 dans le même instantané [S2]	Référence de durée identique
250	Organisations candidates sélectionnées dans treize secteurs [S3]	Classement officiel ou échantillon national représentatif
49 des 250	Organisations avec un identifiant proposé à la vente lors de la vérification [S3]	Comptes validés, ventes conclues ou intrusions confirmées
48 / 100	Indicateur national Atlas pour 247 organisations évaluées [S3]	Prévalence nationale ou évaluation sectorielle
60 475	Publications distinctes retenues pour cette édition [S1]	Ensemble de la cybercriminalité suisse ou incidents uniques
27 128	Signalements volontaires reçus par l'office fédéral au premier semestre 2026 [S5]	Attaques confirmées ou mesure comparable aux publications clandestines
200	Annonces obligatoires dans ce bilan semestriel de l'autorité [S5]	Total exhaustif des cyberincidents suisses
79	Cas suisses de rançongiciels dans les signalements et observations semestriels de l'autorité [S5]	Sous-ensemble directement rapprochable des 122 inscriptions
97 000	Enregistrements approximatifs de l'application dans l'avis cantonal de novembre [S16]	Personnes distinctes ou vol confirmé de chaque pièce jointe

POINTS À RETENIR

01

Traitez séparément annonces, inscriptions et communications officielles.

02

Validez les éléments d'identité et de fournisseur avant de décrire le périmètre d'un incident.

03

Exigez une reprise démontrée et un arbre de décision d'annonce testé.

Carte du rapport

Commencez par votre décision, puis suivez les éléments qui l'étayent et son test de réalisation.

Conseil d'administration et RSSI	Quels risques justifient un investissement immédiat ?	01 05 11 12
SOC et réponse aux incidents	Quand une affirmation externe nécessite-t-elle une enquête ?	04 06 07 12
Identité et infrastructure	Quels accès et dépendances doivent être validés ?	03 05 07 12
Fraude et banque	Quels faits personnels ne doivent jamais autoriser une transaction ?	08 09 12
Juridique et achats	Qui doit annoncer quoi à qui et sous quel régime ?	05 10 12

Catégorie d'éléments	Question traitée	Limite
Publications clandestines	Ce qui est annoncé, recherché ou proposé	Authenticité et résultats exigent des preuves distinctes
Inscriptions de rançongiciels	Ce qui figure dans l'instantané retenu	Les dates d'inscription peuvent différer des dates d'intrusion
Observations passives	Ce que montrent les configurations publiques	Aucune preuve d'intrusion ou d'efficacité des contrôles
Communications officielles	Ce qu'une organisation ou autorité rapporte	Les estimations et enquêtes peuvent évoluer
Évaluations officielles des menaces	Les menaces évaluées par une autorité	L'attribution reste celle de l'autorité

Sommaire et parcours de lecture

Le rapport présente les décisions, puis les éléments qui les étayent et les travaux attribués à des responsables. Lisez les limites associées à chaque chiffre et à chaque cas.

Chapitre	Question	Premier lecteur
1 Synthèse	Quelles décisions découlent des éléments disponibles ?	Direction
2 Contexte numérique et sécuritaire	Quelles dépendances façonnent la situation suisse ?	Direction
3 Exposition des organisations	Que permet d'établir la population sélectionnée ?	Infrastructure
4 Éléments du dark web	Qu'est-ce qui est proposé et reste à vérifier ?	Renseignement sur les menaces
5 Incidents sectoriels	Qu'ont communiqué les organisations et les autorités ?	Responsables sectoriels
6 Hacktivisme et DDoS	Qu'est-ce qui distingue les annonces des interruptions de service ?	Exploitation
7 Acteurs de la menace	Quelles relations et attributions sont étayées ?	Renseignement sur les menaces
8 Économie de la fraude	Comment les fraudeurs utilisent-ils les identités et la confiance ?	Équipes antifraude
9 Banque	Quels contrôles nécessitent une responsabilité commune entre finance et sécurité ?	Banque et identité
10 Réponse réglementaire	Quelles obligations d'annonce s'appliquent à quels événements ?	Juridique et conformité
11 Perspectives	Quels signaux modifieraient l'analyse ?	Direction
12 Plan d'action	Qui agit et qu'est-ce qui démontre la réalisation ?	Tous les responsables

Parcours direction : chapitres 1, 5, 10–12. **Parcours exploitation** : chapitres 4, 6–7 et 12. **Parcours identité et fraude** : chapitres 3, 8–9 et 12.

Observé signifie que le document ou la mesure est disponible. **Affirmé** désigne une déclaration dans une publication ou une inscription. **Rapporté officiellement** désigne une communication d'une organisation ou d'une autorité, dans le périmètre indiqué.

Une interprétation d'analyste relie les éléments disponibles à une décision. Elle ne remplace pas les preuves manquantes sur l'accès, l'attribution, les personnes concernées ou les pertes.

CHAPITRE 02

Contexte numérique et paysage des menaces en Suisse

02

CE CHAPITRE RÉPOND À LA QUESTION

Quelles caractéristiques suisses façonnent les menaces auxquelles la direction doit se préparer ?

3

contextes distincts : informations sensibles, services partagés et événements publics

2.1 La valeur des informations compte davantage que l'étiquette nationale 11
2.2 Les évaluations d'espionnage exigent une attribution explicite 12
2.3 Les services partagés peuvent relier des incidents autrement distincts 13
2.4 L'hébergement ne détermine pas la nationalité de l'opérateur 13
2.5 Les événements internationaux constituent un contexte de préparation à la continuité 14
2.6 Les annonces modifient ce qui peut être compté 14

CHAPITRE 02

Contexte numérique et paysage des menaces en Suisse

EN BREF

La Suisse réunit organisations internationales, instituts de recherche, services financiers et infrastructures numériques partagées. Le Service de renseignement de la Confédération identifie ces milieux comme des cibles de renseignement. Les obligations d'annonce couvrent des services critiques désignés. Les événements internationaux créent aussi des occasions de revendications contre la disponibilité. Ces problèmes exigent des preuves différentes. Identifiez les informations, fournisseurs et dépendances de services essentiels à votre organisation avant de choisir les contrôles.

2.1 La valeur des informations compte davantage que l'étiquette nationale

Le contexte national crée plusieurs motifs distincts de ciblage. L'évaluation 2026 du Service de renseignement de la Confédération cite les autorités, organisations internationales, institutions diplomatiques, entreprises internationales, universités et instituts de recherche parmi les cibles de renseignement [S9]. Il s'agit de l'évaluation du SRC. Elle n'établit pas que chaque organisation de ces catégories a subi un incident pendant la période étudiée.

Pour un responsable de sécurité, la question utile concerne les informations qui conserveraient leur valeur après la perte d'accès. Positions de négociation, résultats de recherche, relations clients et plans opérationnels peuvent nécessiter des protections différentes. Une alerte nationale générique n'y répond pas. Le propriétaire de l'information doit identifier les travaux sensibles et leurs accès.

Le SRC décrit un intérêt particulier pour la politique extérieure, commerciale et sécuritaire, les capacités militaires, l'armement et la recherche avancée [S9]. Cette liste concerne les priorités de renseignement. Une annonce vendant des données clients constitue une proposition distincte, même si le secteur est identique. Aucune population ne permet d'estimer l'autre.

Cette distinction modifie la réponse. Une affirmation concernant des données clients appelle conservation des preuves, validation des enregistrements et préparation antifraude. Un accès suspecté à des recherches sensibles nécessite aussi l'examen des comptes collaboratifs, dépôts de projets et partages externes. Les deux exigent de vérifier le système et la période d'accès concernés. L'étiquette nationale ne les établit pas.

Le tableau relie le contexte national à une question interne, sans attribuer de score de menace à un secteur.

Contexte	Évaluation de la source	Question interne	Responsable
Autorités et diplomatie	Le SRC identifie les informations politiques comme un objectif de renseignement [S9]	Qui peut lire à distance les documents sensibles de préparation ?	Propriétaire de l'information et équipe identité
Universités et recherche	Le SRC cite les institutions scientifiques et les technologies avancées [S9]	Quels collaborateurs externes gardent un accès après la fin du projet ?	Direction de la recherche et informatique
Entreprises internationales	Le SRC inclut les entreprises internationales parmi les cibles de renseignement [S9]	Quelles décisions commerciales dépendent d'informations confidentielles ?	Direction métier et sécurité
Services numériques partagés	Le SRC identifie les télécommunications et fournisseurs informatiques comme des voies d'accès possibles [S9]	Quel fournisseur peut atteindre plusieurs services critiques ?	Achats et responsables de services

2.2 Les évaluations d'espionnage exigent une attribution explicite

La synthèse fédérale 2026 désigne les services russes et chinois comme principale menace d'espionnage en Suisse, aux côtés des cybermenaces étatiques russes, chinoises, iraniennes et nord-coréennes décrites par le SRC [S9][S110]. Cette évaluation officielle associe l'activité russe aux pressions politiques, diplomatiques et sur les infrastructures critiques, et l'activité chinoise à la collecte technologique, économique et scientifique [S9][S110]. Ces attributions appartiennent aux autorités fédérales ; ce rapport n'attribue aucun pays d'origine à une offre de données ou perturbation de site non vérifiée.

La même évaluation identifie l'exploitation d'équipements réseau exposés à Internet, le phishing ciblé et les contacts par messagerie [S9]. Elle indique que les vulnérabilités connues de logiciels obsolètes sont utilisées plus souvent que les vulnérabilités inconnues. Cela justifie de prioriser les responsables d'actifs, les logiciels maintenus et les corrections rapides. Cela n'identifie pas le point d'entrée d'un incident suisse particulier.

La recherche et le développement nécessitent une attention particulière, car leurs informations peuvent conserver longtemps leur valeur. Le SRC inclut les travaux universitaires et la recherche privée dans son évaluation [S9]. Le plan de réponse devrait donc couvrir les accès persistants et partages inappropriés, en plus des interruptions évidentes.

Un examen pratique commence par les systèmes transmettant des travaux sensibles entre organisations. Attribuez un responsable aux accès distants, identités externes, dépôts partagés et canaux d'assistance des fournisseurs. Exigez des preuves de suppression des accès à la fin des relations commerciales. Il s'agit de valider les contrôles, sans affirmer que ces systèmes ont été attaqués.

2.3 Les services partagés peuvent relier des incidents autrement distincts

La dépendance aux fournisseurs relie des processus distincts dans l'organigramme. Le SRC identifie les prestataires informatiques comme des voies d'accès importantes. Il décrit les opérateurs télécoms comme des cibles de renseignement et des voies d'accès possibles aux clients [S9]. La FINMA souligne aussi les scénarios propres à chaque établissement et les dépendances envers les tiers [S61].

Un incident chez un fournisseur peut avoir plusieurs conséquences simultanées. Le personnel peut perdre l'accès à un service alors que les informations clients restent disponibles ailleurs. La reprise peut dépendre du service d'identité, de l'assistance ou d'un sous-traitant du fournisseur. L'accès aux données reste une question distincte de l'arrêt du service.

L'inventaire des services doit donc dépasser le nom du fournisseur. Il doit relier le service à un processus métier, aux informations sensibles, aux modes de travail alternatifs et à un contact d'incident. La preuve de réalisation est une fiche de dépendances testée. Un contrat confiant la sécurité au prestataire ne prouve pas la capacité de reprise.

Dans les établissements financiers, la responsabilité reste également celle de l'établissement surveillé. La communication FINMA précise que la responsabilité des exigences prudentielles ne peut être transférée au prestataire [S8]. Le chapitre 10 explique comment le délai d'annonce peut commencer lorsqu'un prestataire externalisé identifie un incident.

2.4 L'hébergement ne détermine pas la nationalité de l'opérateur

Le SRC décrit l'utilisation d'infrastructures serveurs suisses par des revendeurs et intermédiaires pour des opérations visant l'étranger [S9]. Il explique aussi que les acteurs changent d'infrastructure et utilisent plusieurs systèmes intermédiaires. La localisation suisse d'un serveur n'établit donc ni un opérateur suisse, ni une victime suisse, ni une implication de l'État suisse.

Pour les hébergeurs et fournisseurs cloud, la décision est opérationnelle. Conservez les traces de location et d'administration lorsqu'un incident crédible exige une enquête. Assurez-vous que le service peut identifier la relation client pertinente et répondre par les voies juridiques et sécuritaires établies. Évitez de relier tous les clients d'une infrastructure partagée à l'activité.

Pour les autres organisations, la leçon concerne l'attribution. La localisation réseau peut aider l'enquête, sans établir qui a dirigé l'opération. Une langue, un pays d'hébergement ou un motif politique revendiqué doit rester une observation séparément étiquetée. Une relation entre acteurs exige des preuves de cette relation, au-delà d'une référence nationale commune.

2.5 Les événements internationaux constituent un contexte de préparation à la continuité

Le Sommet sur la paix en Ukraine de juin 2024 est un contexte historique pertinent, extérieur à la période des incidents étudiés. Dans son premier bilan, le NCSC attribuait les activités DDoS autour du sommet à NoName057(16) [S42]. Il signalait de légères perturbations d'infrastructures. Il précisait aussi que les systèmes et données du sommet et de ses organisateurs n'avaient pas été menacés.

La source distingue plusieurs phénomènes. Elle rapportait séparément les tentatives d'intrusion numérique, le phishing et les DDoS. Elle indiquait que les problèmes de diffusion et une panne électrique n'étaient pas des incidents de cybersécurité [S42]. Cette distinction compte lorsque des perturbations techniques surviennent pendant un événement très visible.

Ce bilan historique justifie la préparation aux interruptions de services publics autour des grands événements. Il n'établit pas qu'une campagne semblable a eu lieu en 2026. Le SRC estime séparément très probables les attaques par saturation autour des conférences internationales et grands événements [S9]. Il s'agit de son évaluation, sans prévision propre au rapport ni position sur l'événement.

Utilisez le calendrier événementiel pour exercer la continuité, l'escalade auprès des prestataires et les communications publiques. Une déclaration doit distinguer la revendication de l'acteur, l'impact observé par l'organisation et les inconnues. Ne déduisez pas un accès aux données d'une panne de site. Ne déduisez pas une cause politique de la seule concomitance.

2.6 Les annonces modifient ce qui peut être compté

L'obligation d'annonce des infrastructures critiques a débuté le 1 avril 2025 [S60]. Dans ses bilans semestriels, l'OFCS compte 35 727 signalements combinés au premier semestre 2025 [S108]. Il sépare ensuite 29 006 signalements volontaires et 145 annonces obligatoires au second semestre 2025, contre 27 128 et 200 au premier semestre 2026 [S5][S107]. Une comparaison annuelle doit tenir compte de ce changement terminologique et de l'entrée en vigueur d'avril 2025 avant d'interpréter une tendance [S60][S107][S108]. Ces annonces ne sont pas équivalentes aux publications clandestines, aux inscriptions de rançongiciels ou à tous les incidents subis par les organisations suisses.

Les populations distinctes du rapport doivent orienter les décisions sans être regroupées en un total national. Les avertissements publics peuvent identifier un type de campagne. Une inscription d'extorsion consigne une affirmation. Associations d'exposition et configurations passives décrivent des observations différentes. Chacune nécessite sa validation et son responsable.

Aucune déclaration sur la confidentialité bancaire ou les relations extérieures n'est nécessaire pour transformer ces observations en explication causale. Les questions pertinentes sont les informations concernées, le service touché et ce que les preuves permettent d'établir. Le chapitre 10 traduit les différentes obligations d'annonce en un dossier de décision d'incident.

POINTS À RETENIR

01

Attribuez les évaluations nationales de renseignement au SRC et distinguez-les des affirmations sur des incidents individuels.

02

Les services partagés relient impact métier, reprise et obligations d'annonce ; testez ces dépendances avec le fournisseur.

03

Le bilan du sommet 2024 est historique ; la concomitance et l'interruption d'un site ne prouvent pas un accès aux données.

CHAPITRE 03

Exposition nationale : la population d'organisations sélectionnée

CE CHAPITRE RÉPOND À LA QUESTION

Quelles observations d'identité nécessitent une validation dans les organisations sélectionnées ?

49 des 250

organisations avaient un identifiant proposé à la vente lors de la vérification

3.1 Fiche de population 17

3.2 Observations passives et limites 19

3.3 Annonces actuelles et indicateur national Atlas 20

3.4 Observations d'appareils, d'identifiants et de documents 21

3.5 Transformer un signal externe en décision défendable 23

CHAPITRE 03

Exposition nationale : la population d'organisations sélectionnée

EN BREF

49 des 250 organisations sélectionnées avaient un identifiant proposé à la vente lors de la vérification. Les observations couvrent 247 organisations ; 3 restent non évaluées. L'indicateur national Atlas atteint 48 sur 100 pour ce portefeuille évalué. Associations d'appareils et identifiants historiques peuvent concerner clients, employés ou données anciennes. La configuration passive a son propre dénominateur. Validez les annonces actuelles, examinez les éléments pertinents sur les appareils d'employés et vérifiez les contrôles prévus du courrier et du web.

3.1 Fiche de population

La sélection et la mesure sont distinctes. L'inclusion désigne une organisation candidate à l'évaluation. Elle n'établit ni exposition, ni incident actuel, ni groupe d'entreprises exploité indépendamment [S3].

Élément	Définition
Population sélectionnée	250 organisations candidates avec un domaine public principal
Base de sélection	Autorités publiques, répertoires officiels financiers et éducatifs, organisations sectorielles importantes
Objectif	Décrire certains signaux externes et alimenter les questions aux responsables de services
Couverture	Treize groupes sectoriels
Périmètre organisationnel	Certaines filiales exploitées séparément partagent une société mère
Base temporelle	Exposition lue les 21 et 22 novembre 2026 ; les observations passives ont leur propre date d'instantané
Résultats publics	Nombres sectoriels de signaux et indicateur national Atlas ; organisations individuelles masquées
Limite d'inférence	Aucune estimation de prévalence nationale, aucun classement sécuritaire ni certification des contrôles individuels

Le tableau décrit la population sélectionnée. Ces groupes sont analytiques. Ils ne déterminent pas l'obligation légale d'annonce applicable aux infrastructures critiques d'une organisation.

Secteur	Organisations candidates	Question de défense
Banque et finance	40	Les équipes identité, fraude et paiement peuvent-elles valider le même événement ?
Administration publique	35	Un service peut-il continuer quand une application est isolée ?
Formation et recherche	25	Qui peut exporter des recherches ou des données d'identité par les services partagés ?
Santé	20	Les processus cliniques peuvent-ils continuer pendant la restauration ?
Énergie et services collectifs	20	Quelles dépendances métier peuvent affecter les opérations essentielles ?
Transport et logistique	20	Les processus clients et opérationnels peuvent-ils reprendre séparément ?
Industrie et construction	21	Les accès fournisseurs et dépendances de production sont-ils compris ?
Télécommunications et technologie	15	Qui peut réinitialiser les identités ou publier des communications fiables ?
Sciences de la vie et chimie	15	Quels partenaires traitent les informations de recherche et de personnel ?
Commerce, alimentation et agriculture	15	Quels comptes clients et fournisseurs autorisent les transactions ?
Médias grand public et immobilier	9	Quelles plateformes externalisées détiennent des informations clients ?
Commerce et services aux entreprises	5	Quels services partagés soutiennent les transactions critiques ?
Assurance	10	Peut-on rattacher les dossiers de sinistres et de prévoyance à chaque sous-traitant ?
Total	250	Sélection raisonnée avec différents périmètres institutionnels

3.2 Observations passives et limites

L'instantané passif couvre 246 des 250 domaines candidats sélectionnés, en omettant une organisation dans chacun des secteurs banque et finance, administration publique, formation et recherche, et santé. Ces quatre omissions ne recoupent pas les trois organisations non évaluées de la population d'exposition de 247 organisations, laissant 243 organisations évaluées dans les deux contrôles. Les réponses non concluantes ne sont pas considérées comme des défaillances de contrôle [S3].

Observation	Nombre	Dénominateur
Domaines candidats évalués	246	246
Politique DMARC reject ou quarantine observée	164	246
SPF observé	233	246
Enregistrements DKIM observés	168	246
Enregistrement de délégation DNSSEC observé	69	246
Vérification du certificat TLS valide	243	246
Validation du certificat TLS infructueuse	2	246
Vérification TLS non résolue	1	246
Réponse enregistrée	216	246
HSTS observé	182	216

L'observation de politique de messagerie consigne une politique publiée. Elle ne mesure pas le rejet de chaque message frauduleux. Un enregistrement DKIM ne prouve pas la signature de tous les flux légitimes. Les observations HSTS utilisent le dénominateur des réponses.

Une politique observée constitue une question pour le responsable du service. Une politique limitée à la surveillance peut être intentionnelle pendant l'évaluation des expéditeurs légitimes. Une observation absente peut aussi résulter d'une réponse non concluante. Rien ne prouve ainsi qu'un attaquant a utilisé cette condition.

Pour l'authentification des courriels, le résultat opérationnel essentiel est l'alignement des messages légitimes et l'application possible de la politique prévue par les destinataires. La publication d'une politique ne prouve pas ces résultats. Le responsable doit vérifier les rapports de distribution et les services d'envoi autorisés avant de modifier l'application.

Une observation de délégation DNS décrit les informations de confiance visibles pour ce domaine. Elle n'audite pas chaque résolveur, enregistrement ou service de noms interne. Un certificat TLS valide établit aussi une observation limitée de sécurité du transport. Il n'évalue ni les autorisations applicatives, ni les contrôles de reprise, ni les données clients stockées.

Les observations des en-têtes ont un périmètre encore plus étroit. Un en-tête observé sur une réponse peut différer selon l'application, le nom d'hôte ou le chemin. Vérifiez la cohérence des politiques entre les services importants. Validez ensuite l'expérience utilisateur après toute modification.

Les observations passives décrivent la configuration selon des dénominateurs sectoriels explicites

	DMARC	SPF	DKIM	DNSSEC	TLS	HSTS
Banque et finance	25/39	38/39	19/39	21/39	39/39	34/35
Administration publique	20/34	30/34	12/34	6/34	33/34	24/30
Éducation et recherche	9/24	23/24	21/24	11/24	24/24	16/23
Santé	11/19	17/19	11/19	3/19	19/19	14/19
Énergie et services publics	15/20	19/20	18/20	0/20	20/20	17/19
Transport et logistique	13/20	19/20	15/20	9/20	19/20	15/17
Télécommunications et technologie	15/15	15/15	11/15	4/15	15/15	11/14
Sciences de la vie et chimie	10/15	14/15	13/15	2/15	15/15	9/13
Industrie et construction	17/21	21/21	16/21	5/21	21/21	16/18
Assurance	8/10	10/10	7/10	3/10	10/10	8/8
Commerce, alimentation et agriculture	12/15	14/15	13/15	2/15	14/15	9/10
Services aux entreprises et aux consommateurs	9/14	13/14	12/14	3/14	14/14	9/10

Source : observations passives, 22 novembre 2026. Chaque cellule indique les domaines observés/évalués ; HSTS repose sur les réponses enregistrées. Les politiques publiées ne prouvent pas leur application à chaque message [S3].

3.3 Annonces actuelles et indicateur national Atlas

49 des 250 organisations sélectionnées avaient un identifiant proposé à la vente lors de la vérification. Les observations d'exposition couvrent 247 organisations ; les 3 organisations sans résultat (énergie et services collectifs, transport et logistique, services aux entreprises et aux consommateurs) figurent toutes dans l'instantané passif de 246 domaines. L'indicateur national Atlas atteint 48 sur 100 pour le portefeuille évalué [S3].

Des valeurs Atlas plus élevées indiquent une exposition observée plus forte. L'indicateur décrit le portefeuille sélectionné, sans mesurer la prévalence nationale ni compter des incidents confirmés. Ce rapport publie uniquement ce chiffre national Atlas. Le tableau sectoriel présente les nombres de signaux, avec chaque population évaluée visible.

Les tableaux d'exposition et d'observations passives regroupent les services aux entreprises et aux consommateurs. La fiche de population conserve les secteurs de sélection initiaux.

Secteur	Évaluées	Annonces actuelles	Appareils employés : organisations	Documents : organisations	Appareils : organisations
Banque et finance	40	7	15	19	36
Administration publique	35	4	20	26	29
Éducation et recherche	25	6	23	24	25
Santé	20	0	10	6	14
Énergie et services collectifs	19	1	10	8	15
Transport et logistique	19	7	14	10	17
Télécommunications et technologie	15	6	13	13	15
Sciences de la vie et chimie	15	2	12	10	12
Industrie et construction	21	4	16	16	18
Assurance	10	3	7	8	10
Commerce, alimentation et agriculture	15	6	10	9	14
Services aux entreprises et aux consommateurs	13	3	8	9	10
Toutes évaluées	247	49	158	158	215

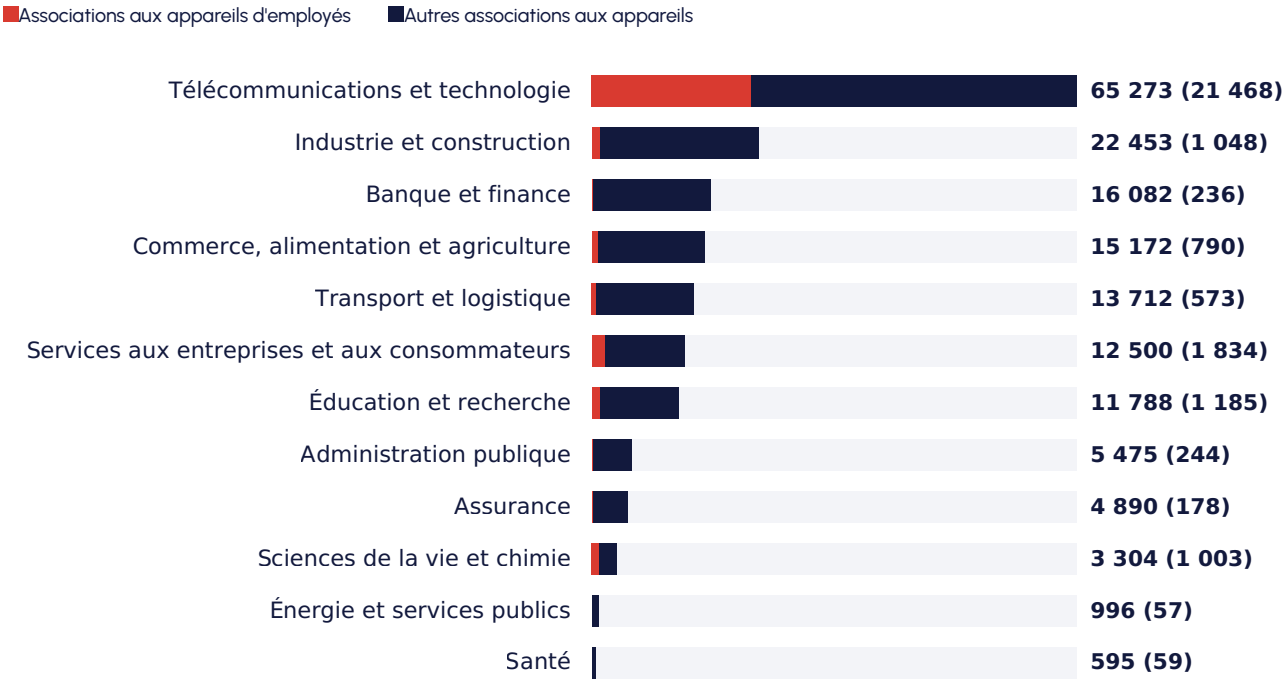
Une annonce actuelle signifie qu'un identifiant associé au domaine était proposé lors de la vérification. Elle n'établit ni validité du compte, ni vente conclue, ni accès aux systèmes internes. Conservez l'offre et validez le compte dans les registres autorisés de l'organisation.

3.4 Observations d'appareils, d'identifiants et de documents

L'instantané d'exposition a été lu les 21 et 22 novembre 2026. Les totaux d'appareils et d'identifiants décrivent les enregistrements alors disponibles, dont des données anciennes. Les mentions couvrent les 365 jours précédents ; les domaines ressemblants couvrent 30 jours [S3].

Observation	Nombre	Organisations évaluées
Associations d'appareils, au moins	172 240	247
Associations d'appareils classés employés	28 675	247
Autres associations d'appareils	143 565	247
Associations historiques d'identifiants	11 072 599	247
Enregistrements de bases de données divulguées	4 102 097	247
Lignes de journaux de logiciels voleurs	2 216 250	247
Entrées de listes d'identifiants	4 754 252	247
Observations de domaines ressemblants	109 410	247
Observations documentaires	2 696	247

Associations d'appareils et d'identifiants dans les populations sectorielles évaluées



Source : observations d'exposition pour 247 organisations candidates évaluées, 21-22 novembre 2026. Associations cumulatives, sans preuve d'intrusion vérifiée [S3].

Certains totaux d'appareils sont des minima. Ce sont des associations à des domaines sélectionnés, pas des personnes ou employés suisses distincts. Un appareil ou identifiant peut être associé à plusieurs organisations. Les enregistrements peuvent être répétés, obsolètes ou déjà corrigés.

Les associations classées comme appareils d'employés nécessitent une validation des comptes actuels et appareils gérés. Les associations hors de cette catégorie n'établissent pas la propriété de l'appareil. Les domaines éducatifs et de services clients peuvent inclure étudiants, clients et autres utilisateurs autorisés.

Des noms de domaines similaires ne prouvent seuls ni phishing ni intention malveillante. Les observations documentaires exigent de vérifier séparément propriété, accessibilité et sensibilité. Distinguez ces examens des mesures de confinement des comptes.

3.5 Transformer un signal externe en décision défendable

Les équipes d'identité doivent établir si le compte ou service appartient à l'organisation, reste actif et bénéficie d'une correction antérieure couvrant les mêmes éléments. Le renseignement sur les menaces doit conserver l'annonce séparément des constats internes.

Examinez sessions, changements de récupération, autorisations d'applications et règles de messagerie. Décrivez l'absence de télémétrie correspondante avec ses limites de conservation et de couverture. Un ancien mot de passe retiré peut justifier une clôture ; une session non autorisée peut exiger révocation et escalade.

Une association à un domaine bancaire peut concerner client, employé, fournisseur ou enregistrement historique. Le chapitre 9 distingue le groupe bancaire complet du sous-ensemble rapproché des émetteurs. Aucune population n'établit un taux de compromission bancaire.

Consignez responsable, observations, incertitude, action et condition de réouverture. Demandez au responsable métier de démontrer la continuité si un service est isolé. Validation des comptes, assurance de configuration et reprise nécessitent chacune leurs preuves de clôture.

POINTS À RETENIR

01

Validez les annonces actuelles contre les comptes actifs et comportements pertinents.

02

Distinguez les associations cumulées des personnes et incidents actuels.

03

Lisez résultats d'exposition et observations passives avec leurs différents dénominateurs évalués.

CHAPITRE 04

Offres du dark web et limites des éléments disponibles

04

CE CHAPITRE RÉPOND À LA QUESTION

Que prouvent les offres clandestines liées à la Suisse et où chercher des corroborations ?

5

études de cas distinguant données annoncées et incidents vérifiés

4.1 Population observée 25

4.2 Des produits différents exigent des réponses différentes 28

4.3 Cinq cas à valider 29

4.4 Identifiants, contacts et demande 35

4.5 Activité récente : 9–22 novembre 38

4.6 Relier les éléments à une décision attribuée 39

CHAPITRE 04

Offres du dark web et limites des éléments disponibles

EN BREF

Les publications liées à la Suisse proposent dossiers d'assurance, informations clients, contacts et accès aux comptes. Certaines décrivent des données anciennes ; d'autres sont des demandes d'achat ou des réponses citant une affirmation. Une offre concernant un prestataire ajoute la sécurité physique aux questions de réponse. Aucune annonce ne prouve seule une intrusion, une vente conclue ou un accès actuel. Validez source, date, compte et processus métier avant le confinement ou la communication d'un nombre de personnes concernées.

4.1 Population observée

Une étiquette nationale ne prouve pas une victime suisse. Odin by Brandefense a compté 59 956 publications portant une étiquette suisse pendant la période indiquée. L'ensemble retenu comprend 60 475 publications distinctes dans les populations de sources du rapport. Ces chiffres décrivent des publications, sans compter incidents, personnes ou transactions réussies. [S1]

Les populations de sources se chevauchent. Le total combiné est une population distincte ; ces lignes ne doivent donc pas être additionnées. La couverture retenue est incomplète lorsque les documents sources étaient indisponibles.

Population	Publications	Signification
Total portant une étiquette nationale	59 956	Population de publications rapportée pour la période
Documents retenus avec étiquette nationale	59 953	Documents disponibles pour cette édition
Documents de forums retenus	1409	Documents de forums retenus concernant la Suisse
Documents récents retenus	1595	Publications datées du 9–22 novembre
Ensemble retenu	60 475	Publications distinctes dans les populations de sources

Les totaux par plateforme avec étiquette nationale décrivent les lieux de publication. Ils ne comptent ni personnes uniques, ni groupes criminels, ni transactions réussies [S1].

Plateforme	Publications	Limite
Telegram	58 805	Publications, sans participants uniques
Forum	887	Publications, sans participants uniques
Discord	240	Publications, sans participants uniques
Paste	24	Publications, sans participants uniques
Tor	0	Publications, sans participants uniques

Les étiquettes linguistiques décrivent les documents. Elles n'établissent ni citoyenneté de l'auteur, ni localisation de l'acheteur, ni identité de l'attaquant. Plusieurs étiquettes peuvent s'appliquer à une publication [S1].

Langue	Publications étiquetées	Interprétation
Anglais	35 077	Observation linguistique sans attribution
Allemand	585	Observation linguistique sans attribution
Français	492	Observation linguistique sans attribution
Italien	95	Observation linguistique sans attribution
Russe	5 835	Observation linguistique sans attribution
Turc	2 039	Observation linguistique sans attribution

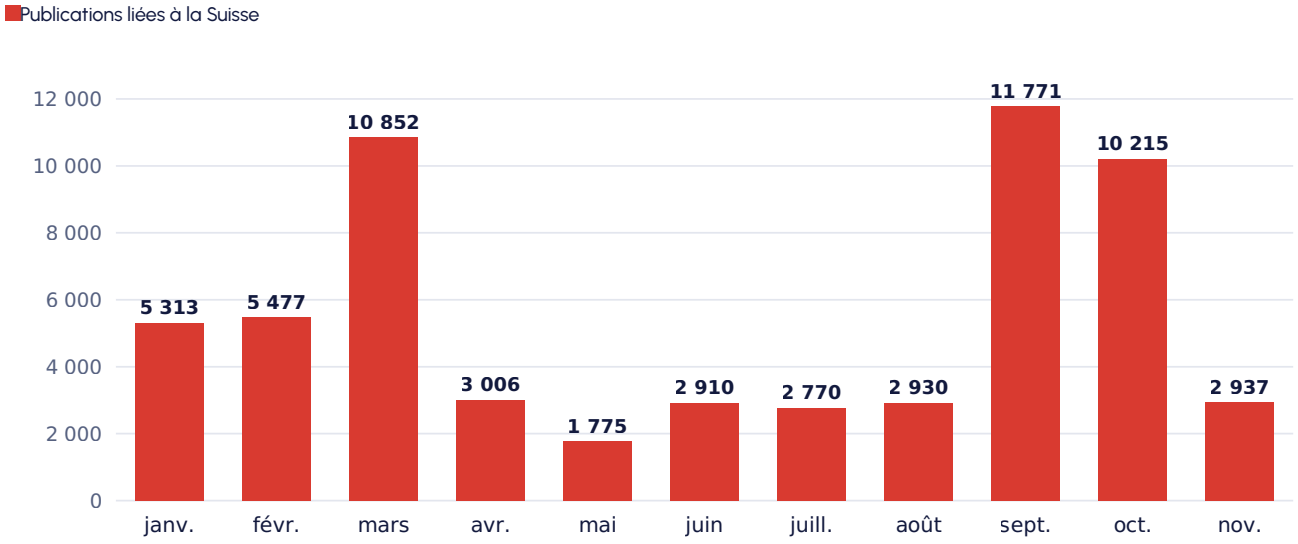
Le graphique mensuel conserve l'unité de publication. Les annonces automatisées et répétées peuvent influencer le volume. Le graphique aide donc l'examen des éléments, sans conclure à une croissance des attaques.

La distinction compte, car la Suisse apparaît dans différents documents. Un vendeur peut inclure le pays dans un stock mondial. Un acheteur peut demander des informations suisses sans rien proposer. Une réponse de forum peut répéter une allégation antérieure. Une publication peut aussi décrire un service basé ailleurs ou un ancien incident concernant une marque suisse internationale.

Les cas commencent donc par la proposition réellement étayée par chaque publication. Une annonce établit qu'une offre a été observée. Une citation dans une réponse établit que le participant a répété l'affirmation. Une demande d'échantillon établit une question de vérification ouverte. Rien ne fournit ainsi de preuve forensique du côté de la victime.

Les termes de fraîcheur exigent aussi de la retenue. Les mentions telles que « frais » peuvent décrire un produit reconditionné, une annonce récente ou une affirmation sur les données sous-jacentes. Elles n'établissent ni la date du vol ni la validité actuelle du compte. La question défensive est la correspondance avec un compte, processus ou ensemble de données encore utilisé.

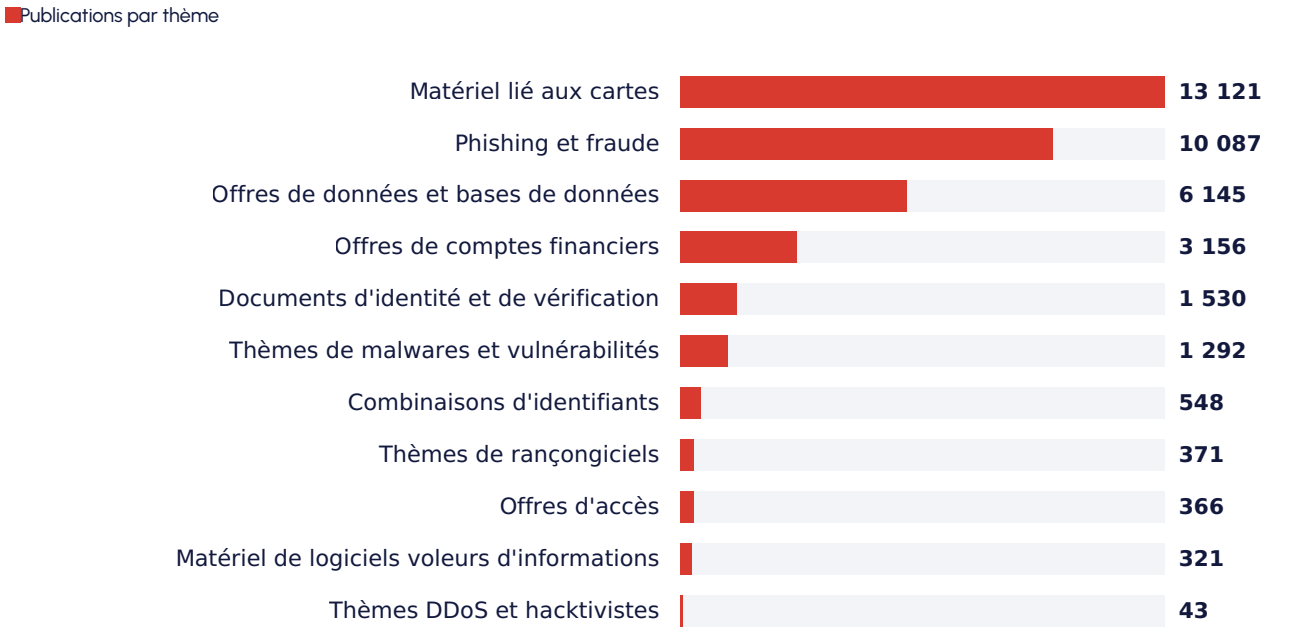
Le volume des publications liées à la Suisse varie sans mesurer la fréquence des incidents



Source : publications retenues liées à la Suisse, 1 janvier-22 novembre 2026 à 07:20 UTC ; novembre partiel. Les thèmes peuvent se chevaucher ; les publications ne sont pas des incidents confirmés [S1].

Les totaux thématiques décrivent des documents retenus avec chevauchement. Les publications concernant les cartes ne mesurent ni cartes ni pertes. Utilisez le graphique pour attribuer les examens, sans déduire un marché national de fraude [S1].

Les thèmes liés aux cartes sont fréquents dans les publications retenues



Source : publications retenues liées à la Suisse, 1 janvier-22 novembre 2026 à 07:20 UTC ; novembre partiel. Les thèmes peuvent se chevaucher ; les publications ne sont pas des incidents confirmés [S1].

4.2 Des produits différents exigent des réponses différentes

Le tableau regroupe les éléments sélectionnés selon la décision de réponse possible. Ses lignes sont des exemples, sans constituer des totaux nationaux mutuellement exclusifs de criminalité. [S1]

Documents	Observation	Limite principale	Première décision
Exports d'assurance	Offre décrivant des lignes contractuelles et deux fichiers	Les lignes ne sont pas des assurés uniques ; provenance non vérifiée	Rapprocher les champs contractuels et les exports autorisés
Données télécoms	Réponses conservant une affirmation volumineuse sur des données clients	La citation et les demandes de preuve ne confirment pas un incident	Chercher des preuves chez le prestataire avant d'utiliser le total annoncé
Informations de prestataire	Offre décrivant des données de gestion d'installations	Validité des informations d'entrée et accès actuel non établis	Réunir fournisseur, cybersécurité et sécurité physique
Personnel des services de soins	Offre décrivant des données du personnel et de gestion	Données de patients, authenticité et accès actuel non vérifiés	Valider séparément les systèmes du personnel et de gestion
Données d'entreprises de transport	Offre décrivant des dossiers clients, salariaux et financiers	Origine, ancienneté et accès actuel non vérifiés	Vérifier les dossiers de gestion et les corrections antérieures
Documents commerciaux historiques	Publication ultérieure décrivant un ancien rançongiciel	Publication et intrusion n'ont pas la même date	Comparer les documents aux corrections antérieures
Exports de sites hébergés	Offre alléguant une cause commune à plusieurs sites	Cause technique commune affirmée sans démonstration	Demander au prestataire et aux clients de valider leurs systèmes
Combinaisons d'identifiants	Annonce de courriels et mots de passe étiquetés suisses	Pays et « frais » ne prouvent pas la validité actuelle	Valider les comptes par les procédures d'identité autorisées
Coordonnées	Annonces de segments téléphoniques ou d'annuaires étiquetés suisses	Origine, âge et personnes uniques non résolus	Préparer le personnel aux usurpations convaincantes utilisant ces contacts
Demandes d'achat	Publications recherchant bases, messageries ou comptes	La demande ne prouve ni possession ni transaction conclue	Utiliser la demande comme contexte de protection des comptes

La bonne réponse peut différer malgré des champs annoncés similaires. Les informations d'assurance nécessitent un examen des contrats et du service client. Les informations d'installations ajoutent un responsable de sécurité physique. Une affirmation d'identifiants historiques appelle une vérification des corrections antérieures avant toute nouvelle campagne de réinitialisation.

4.3 Cinq cas à valider

A

CAS A

Dossiers d'assurance annoncés comme suisses

Fiche de preuve B01 | 4 mai 2026 | Forum de partage de données | Assurance

Partage de données non vérifié

AFFIRMATION	Une publication du 4 mai présentait deux fichiers comme des informations d'assurance suisses. Elle affirmait qu'un fichier contenait 4 260 757 lignes structurées sur les contrats, assurés, véhicules, intermédiaires et détails financiers. [S1]
CHRONOLOGIE	Le même pseudonyme figurait dans deux publications retenues aux formulations très proches le 4 mai. Cela montre une répétition du langage publicitaire, sans établir deux incidents indépendants.
ÉLÉMENTS DISPONIBLES	Le texte décrit des champs contractuels et propose des liens omis ici. L'unité annoncée est une ligne de fichier. Ce n'est pas un nombre vérifié d'assurés ou de contrats uniques.
AUTRES EXPLICATIONS	Versions contractuelles, détails d'assurés répétés et exports administratifs combinés pourraient expliquer les répétitions. Des données historiques reconditionnées, une mauvaise étiquette ou une offre inexacte restent possibles. La publication seule ne tranche pas.
LIMITES	Le rapport n'établit ni contenu, ni provenance, ni âge, ni authenticité des fichiers. Il ne confirme aucune intrusion chez l'assureur, aucun accès actuel ni transfert achevé à un tiers.
RÉPONSE	Les équipes sécurité, protection des données et exploitation devraient comparer toute alerte autorisée à leurs schémas d'export et dossiers de conservation. Confirmez le processus métier avant d'annoncer un total de personnes ou de modifier l'authentification client.

En définitive

Validez provenance et périmètre contractuel avant de transformer les lignes annoncées en personnes touchées.

Une description crédible des champs peut orienter une enquête. Elle ne peut authentifier tout le fichier. La validation doit établir le système producteur, les dates couvertes et les répétitions d'une personne ou police.

Fiche de preuve B01 — 4 mai 2026

NormalLeVrai | Forum de partage de données | Forum | Anglais

ORIGINAL

contains 4,260,757 complete lines of structured insurance data [...] information for a contract [...] related to insurance contracts (policies)

TRADUCTION

(traduction) contient 4 260 757 lignes complètes de données d'assurance structurées [...] informations pour un contrat [...] liées aux contrats d'assurance (polices)

Ce que nous pouvons établir

Offre décrivant deux fichiers comme des informations d'assurance suisses, avec un total de lignes annoncé et des descriptions de champs.

Ce qui n'est pas établi

Fichiers, total de lignes, provenance, personnes uniques, validité actuelle, date d'intrusion ou transfert achevé.

B

CAS B

Allégation télécom dans une réponse (B02, B03)

Télécommunications

Affirmation citée dans des réponses

AFFIRMATION	Une réponse du 10 mars citait une offre attribuée à Niphra. Elle alléguait un incident de janvier 2026 chez un opérateur télécom et annonçait plus de 6 millions d'éléments de données clients. [S1]
CHRONOLOGIE	Un autre participant demandait des échantillons le même jour. La discussion conservait l'allégation et la demande de preuves. Les dates établissent la discussion observée, sans dater l'intrusion alléguée.
ÉLÉMENTS DISPONIBLES	Les pièces présentées sont une citation dans une réponse et une contestation ultérieure. Elles sont moins solides qu'une offre originale authentifiée, un échantillon vérifié ou une déclaration de l'organisation.
AUTRES EXPLICATIONS	Le participant pourrait répéter une offre réelle, copier une allégation infondée ou discuter de données mal étiquetées. La demande de preuves ne démontre pas que l'affirmation est fausse.
LIMITES	Le total annoncé, les champs, l'origine et la date restent non vérifiés. La discussion n'établit ni accès actuel ni incident officiellement confirmé. Elle ne doit pas être ajoutée aux cas confirmés du chapitre 5.

RÉPONSE

Transmettez l'affirmation aux contacts sécurité et protection des données du prestataire par un canal établi. Demandez le périmètre confirmé et les consignes clients. Précisez dans les notes internes quelles informations viennent d'un participant de forum.

En définitive

Une demande d'échantillons conserve une lacune ouverte ; elle ne confirme ni ne réfute l'offre.

Une réponse sceptique prouve un doute, sans constituer un verdict. Prendre une demande d'échantillons pour une réfutation serait aussi injustifié que prendre l'allégation citée pour une confirmation. Gardez la question ouverte tout en vérifiant les éléments auprès de l'organisation responsable.

Fiche de preuve B02 — 10 mars 2026

john2samira, quoting Niphra | Réponse de forum citant une offre | Forum | Anglais

ORIGINAL

Date of breach: January 2026. [...] [telecommunications provider] [...] 6M+ Customer Details [...] please post some rows

TRADUCTION

(traduction) Date de la violation : janvier 2026. [...] [opérateur télécom] [...] 6M+ détails clients [...] veuillez publier quelques lignes

Ce que nous pouvons établir
Réponse conservant une affirmation publicitaire de données clients et demandant des exemples de lignes.

Ce qui n'est pas établi
Déclaration originale authentifiée du vendeur, total client vérifié, propriété des fichiers, accès actuel ou incident confirmé par le prestataire.

Fiche de preuve B03 — 10 mars 2026

jb75 | Discussion de forum | Forum | Anglais

ORIGINAL

Please add a sample. [...] no one can take your word for it if they can't verify the data.

TRADUCTION

(traduction) Veuillez ajouter un échantillon. [...] personne ne peut vous croire sur parole sans pouvoir vérifier les données.

Ce que nous pouvons établir
Un participant contestait les preuves de l'affirmation télécom.

Ce qui n'est pas établi
Preuve de fausseté, validation technique des données alléguées ou confirmation indépendante du vendeur.

CAS C

C ■ Informations de prestataire et questions de sécurité physique

Offre de données de prestataire non vérifiée

Fiche de preuve B04 | 5 nov. 2026 | Forum de vente de données | Services aux entreprises

AFFIRMATION

Une annonce du 5 novembre décrivait une base issue d'un prestataire suisse de services aux entreprises. Elle annonçait 980 093 lignes structurées concernant installations, collecte, logistique et gestion de sites. [S1]

CHRONOLOGIE	La publication observée proposait une vente exclusive. Elle précisait aussi que l'annonceur n'avait pas vérifié chaque ligne. Aucune déclaration ne prouve qu'il contrôlait un ensemble complet ou actuel de données.
ÉLÉMENTS DISPONIBLES	L'annonce relie des informations détenues par un prestataire à plusieurs types d'installations clientes. Son texte est conservé en privé. Descriptions identifiantes, coordonnées et prétendues informations d'entrée sont omises de la fiche publique.
AUTRES EXPLICATIONS	Les données pourraient inclure des consignes périmées, doublons opérationnels, informations de livraison ordinaires ou champs mal décrits. Même un export administratif authentique exigerait une évaluation distincte de son importance actuelle pour la sécurité.
LIMITES	Le rapport ne confirme ni total de lignes, ni informations d'entrée fonctionnelles, ni entrée réussie, ni incident actuel chez le prestataire, ni vente. Les descriptions de clients sensibles ne prouvent pas leur implication.
RÉPONSE	La gestion fournisseurs doit établir les consignes détenues par le prestataire. La sécurité physique doit valider les détails opérationnels correspondants dans ses propres dossiers. Retirez les consignes concernées lorsque leur authenticité et leur usage actuel sont établis.

En définitive

Réunissez cyber et sécurité physique sans présumer que les informations d'entrée annoncées fonctionnent.

La réponse doit inclure le responsable du processus physique. Une équipe cyber peut reconnaître un export client sans voir que les champs opérationnels sont gérés par les équipes immobilières. Une description spectaculaire du vendeur ne doit pas conduire à supposer une entrée réussie dans les locaux.

Fiche de preuve B04 — 5 nov. 2026

pfavre | Forum de vente de données | Forum | Anglais

ORIGINAL

Complete database from a [business-services provider]. [...] 980,093 structured rows [...] we have not manually verified every single row.

TRADUCTION

(traduction) Base complète d'un [prestataire de services aux entreprises]. [...] 980 093 lignes structurées [...] nous n'avons pas vérifié manuellement chaque ligne.

Ce que nous pouvons établir

Annonce revendiquant un ensemble de données de prestataire avec informations de gestion d'installations et total de lignes affirmé.

Ce qui n'est pas établi

Fichier, accès physique actuel, identifiants d'entrée fonctionnels, total de lignes annoncé ou vente réussie.

CAS D

D

Données commerciales antérieures annoncées pendant la période

Documents anciens annoncés à nouveau

Fiche de preuve B05 | 11 oct. 2026 | Forum de partage de données | Commerce

AFFIRMATION	Une publication du 11 octobre proposait des informations associées à un détaillant d'articles de plein air. Elle décrivait un événement de rançongiciel en 2025 et une date estimée antérieure. Ces affirmations historiques restent celles de l'auteur. [S1]
CHRONOLOGIE	Des descriptions similaires figuraient dans une publication retenue de février sous un autre pseudonyme. Celle d'octobre constitue donc une nouvelle observation publicitaire. Elle n'établit pas une nouvelle intrusion en octobre.
ÉLÉMENTS DISPONIBLES	Les publications décrivent des sujets similaires et renvoient à des documents antérieurs. Cela relie leurs récits, sans prouver des fichiers identiques, un transfert entre pseudonymes ou un opérateur commun.
AUTRES EXPLICATIONS	Un auteur peut avoir copié une description, reconditionné des informations anciennes ou obtenu des données indépendamment. Le texte disponible ne tranche pas ces possibilités et n'authentifie pas l'attribution historique revendiquée.
LIMITES	Le rapport ne confirme ni contenu, ni exhaustivité, ni affirmations sur l'incident historique. Il n'établit pas qu'un identifiant décrit reste utilisable. Une publication 2026 ne doit pas devenir, par répétition, un rançongiciel confirmé de 2026.
RÉPONSE	Comparez toute information correspondante aux anciens dossiers d'incident et de correction. Vérifiez la pertinence actuelle des comptes, secrets, accès fournisseurs ou exports conservés. Rouvrez un problème de contrôle lorsque des éléments actuels le justifient.

En définitive

Une date de publication 2026 peut décrire des données anciennes sans établir de nouvelle intrusion.

Les informations historiques peuvent encore nécessiter une protection actuelle. Leur valeur défensive dépend de ce qui reste valide, sans dépendre de la dernière date publicitaire. Le dossier de clôture doit distinguer les données déjà corrigées d'un problème nouvellement validé.

Fiche de preuve B05 — 11 oct. 2026

updap | Forum de partage de données | Forum | Anglais

ORIGINAL

Today I've uploaded [outdoor retailer] [...] DataCarry attack (2025): [...] The estimated compromise date [...] remains unconfirmed by [outdoor retailer].

TRADUCTION

(traduction) Aujourd'hui, j'ai téléversé [détaillant de plein air] [...] attaque DataCarry (2025) : [...] la date estimée de compromission [...] reste non confirmée par [détaillant de plein air].

Ce que nous pouvons établir

Republication décrivant explicitement les données annoncées comme liées à un incident antérieur.

Ce qui n'est pas établi

Nouvelle intrusion 2026, attribution historique affirmée, âge ou exhaustivité des fichiers, ou validité inchangée des identifiants.

CAS E

E

Exports de sites hébergés et cause commune affirmée

Fiche de preuve B10 | 30 janv. 2026 | Forum de partage de données | Services hébergés

Affirmation d'hébergement partagé non vérifiée

AFFIRMATION	Une publication du 30 janvier alléguait une configuration commune d'accès aux bases de plusieurs sites suisses. Elle annonçait 92 fichiers SQL et un ensemble de 45 MB. Une autre réponse de forum répétait cette affirmation. [S1]
CHRONOLOGIE	Les observations retenues situent l'offre et sa répétition dans la période étudiée. Elles ne datent indépendamment aucune intrusion sous-jacente ni création des fichiers.
ÉLÉMENTS DISPONIBLES	Le texte relie plusieurs sites par une explication technique affirmée. La fiche publique omet sites, noms de fichiers et identifiants allégués. Le total de fichiers annoncé n'est pas un nombre vérifié d'organisations.
AUTRES EXPLICATIONS	L'annonce pourrait combiner exports sans lien, sauvegardes historiques ou associations trompeuses de sites. Un hébergement partagé peut expliquer une relation sans établir le même défaut ou accès pour chaque client.
LIMITES	Le rapport n'authentifie ni fichiers ni cause technique alléguée. Il ne confirme pas que tous les sites étaient touchés, qu'un accès aux bases restait disponible ou qu'un opérateur commun avait produit les documents.

RÉPONSE

L'hébergeur et les responsables clients devraient valider leurs traces d'accès, interfaces administratives et historiques d'export. Gardez séparés les résultats de chaque client jusqu'à ce que les preuves étayent une cause commune.

En définitive

Une cause commune exige des preuves du prestataire et des clients au-delà d'annonces similaires.

Une hypothèse de service partagé peut améliorer l'orientation sans devenir une cause racine vérifiée. Le prestataire peut posséder la plateforme administrative, le client la configuration applicative et les données. L'enquête exige un responsable de chaque côté et un dossier commun de faits établis.

Fiche de preuve B10 — 30 janv. 2026

hexvior | Forum de partage de données | Forum | Anglais

ORIGINAL

Multiple Swiss Sites [...] Total Package Size: 45 MB [...] 92 .sql files

TRADUCTION

(traduction) Plusieurs sites suisses [...] Taille totale : 45 MB [...] 92 fichiers .sql

Ce que nous pouvons établir

Affirmation associant plusieurs sites hébergés à des exports de bases annoncés ; une autre réponse répétait l'affirmation.

Ce qui n'est pas établi

Intrusion réussie, cause technique commune, fichiers identiques, nombre d'organisations touchées ou accès actuel aux bases.

4.4 Identifiants, contacts et demande

Les demandes d'achat ne prouvent pas des achats réussis. Une demande de janvier recherchait des bases récentes liées aux cryptomonnaies en Suisse, Allemagne et Autriche. Elle demandait preuves d'âge et exemples de lignes. Elle établit une préférence d'achat déclarée, sans identifier un incident chez une plateforme suisse. [S1]

Une annonce d'avril recherchait des messageries ou comptes liés à la Suisse et indiquait un paiement par compte validé. Les passages russes et anglais ne décrivent pas exactement la même chose. Cette incohérence limite l'interprétation précise de la transaction proposée. Aucun paiement ni contrôle de compte n'a été vérifié. [S1]

Fiche de preuve B06 — 6 janv. 2026

xmrlover76 | Demande d'achat sur forum | Forum | Anglais

ORIGINAL

interested in purchasing [...] Switzerland Crypto DBs [...] must contain minimum 5k+ lines [...] must be able to provide proof

TRADUCTION

(traduction) souhaite acheter [...] bases crypto suisses [...] doivent contenir au minimum 5k+ lignes [...] doit pouvoir fournir des preuves

Ce que nous pouvons établir
Demande d'achat citant la Suisse parmi d'autres pays et exigeant des preuves d'âge des données.

Ce qui n'est pas établi
Données proposées, achat réussi, plateforme d'échange touchée ou intrusion suisse actuelle.

Fiche de preuve B11 — 17 avr. 2026

kleinanzeige | Forum d'achat de comptes | Forum | Russe et anglais

ORIGINAL

Почты на других швейцарских доменах и корпы также принимаются ОПЛАТА - 8$ ЗА 1 ВАЛИДНЫЙ АККАУНТ

TRADUCTION

(traduction) Les messageries sur d'autres domaines suisses et les comptes d'entreprise sont aussi acceptés. PAIEMENT : $8 pour un compte valide.

Ce que nous pouvons établir
Annonce d'acheteur recherchant messageries ou comptes liés à la Suisse et indiquant un prix.

Ce qui n'est pas établi
Transaction achevée, contrôle actuel d'un compte, paiement fiable ou concordance des passages russes et anglais du message complet.

Les combinaisons d'identifiants posent un autre problème d'unité. Une annonce de janvier étiquetait un fichier « Switzerland » et annonçait plus de 24 mille lignes de courriels et mots de passe. Elles peuvent contenir doublons, comptes inactifs, mots de passe réutilisés ou associations nationales erronées. La fraîcheur annoncée ne fournit aucune validation indépendante des comptes. [S1]

La séquence défensive doit commencer dans le processus d'identité autorisé de l'organisation. Vérifiez l'existence du compte, les corrections antérieures et les préoccupations actuelles de connexion. Une réponse perturbatrice doit suivre un risque validé, sans se fonder sur une taille de fichier annoncée.

Fiche de preuve B07 — 27 janv. 2026

thejackal101 | Forum de partage d'identifiants | Forum | Anglais

ORIGINAL

Database: Switzerland [...] Email : Password [...] [24 K++] Line Status: FRESH | HQ

TRADUCTION

(traduction) Base : Switzerland [...] Courriel : Mot de passe [...] [24 K++] Statut des lignes : FRAIS | HQ

Ce que nous pouvons établir
Annonce d'identifiants étiquetés suisses avec total de lignes annoncé et mention de fraîcheur du vendeur.

Ce qui n'est pas établi
Comptes uniques, mots de passe utilisables, résidence suisse, date de vol ou nouvelle organisation touchée.

Fiche de preuve B09 — 18 janv. 2026

Cod3xx | Forum de partage de données | Forum | Anglais

ORIGINAL

Country : Switzerland Format : csv [...]

TRADUCTION

(traduction) Pays : Suisse Format : csv [...]

Ce que nous pouvons établir
Publication proposant un export de contacts étiquetés suisses et décrivant sa structure.

Ce qui n'est pas établi
Méthode d'obtention, intrusion dans des systèmes privés, exhaustivité, accès actuel ou nombre de personnes concernées.

Les données téléphoniques et d'annuaire peuvent faciliter des usurpations convaincantes sans établir un accès au réseau interne. Une annonce du 7 novembre étiquetait un segment « Switzerland-600k », avec des données couvrant 2024–2026 et de nombreux pays. La même affirmation figurait sous différents pseudonymes. La correspondance des mots ne prouve ni fichiers identiques ni opérateur commun. [S1]

Connaître l'employeur, la fonction ou le contrat d'un contact peut donner de la crédibilité. Les équipes clientèle et finance doivent pourtant vérifier indépendamment les changements de compte, paiements et demandes de documents. L'annonce d'une liste de contacts ne confirme pas l'usage de ces données dans une fraude.

Fiche de preuve B08 — 7 nov. 2026

RummRif | Forum de vente de données | Forum | Anglais

ORIGINAL

Year: 2024-2026 Country: [...] *Switzerland-600k [...] & from more 70+ Country.

TRADUCTION

(traduction) Année : 2024-2026 Pays : [...] *Switzerland-600k [...] et de plus de 70+ pays.

Ce que nous pouvons établir
Annonce multinationale de données téléphoniques étiquetant un segment suisse et datant les documents sur plusieurs années.

Ce qui n'est pas établi
Personnes suisses uniques, attribution fiable de chaque numéro, consentement, vol en 2026 ou fraude accomplie.

4.5 Activité récente : 9–22 novembre

La période récente observe des publications. Elle ne compte pas séparément de nouvelles organisations touchées. Les documents anciens réapparaissant à ces dates restent anciens, sauf preuve d'un incident différent.

Une publication de données annoncée n'est pas une fuite accomplie. Un message du 19 novembre affirmait qu'un ancien employé diffuserait des informations bancaires le 30 novembre. Cette date promise dépasse l'arrêté du rapport. Le message ne prouve ni l'emploi, ni la possession d'un fichier, ni un accès actuel. [S1]

Le récit d'une personne interne et les contenus proposés restent les affirmations de l'auteur. Le rapport ne les authentifie pas et n'identifie pas la banque. L'annonce ne doit devenir ni incident confirmé ni diffusion accomplie dans la synthèse, la chronologie ou les totaux bancaires.

La réponse proportionnée est de conserver l'annonce et de la transmettre au processus de sécurité établi. Comparez les preuves obtenues indépendamment aux accès autorisés et aux dossiers de départ. Décidez d'une escalade selon les éléments actuels, en préservant la confidentialité de l'examen.

Fiche de preuve B12 — 19 nov. 2026

Jlkrumholz01 | Annonce de forum | Forum | Anglais

ORIGINAL

On November 30th I will release a PDF list containing all this information. [...] Wait until November 30th. [...] Account Holder Info.

TRADUCTION

(traduction) Le 30 novembre, je publierai une liste PDF contenant toutes ces informations. [...] Attendez le 30 novembre. [...] Informations sur les titulaires de comptes.

Ce que nous pouvons établir
Publication du 19 novembre annonçant une diffusion future de données bancaires après l'arrêté du rapport.

Ce qui n'est pas établi
Emploi revendiqué, possession d'un fichier, accès actuel, authenticité des données, personnes concernées ou diffusion achevée.

Une annonce de service du 19 novembre citait aussi la Suisse parmi ses destinations de voix et messagerie. Elle revendiquait des vérifications d'identité minimales et la conservation des informations d'identité de l'appelant. Des formulations proches sont apparues ensuite. L'annonce ne vérifie ni ces capacités ni leur fonctionnement dans un réseau suisse. [S1]

Cette annonce peut alimenter un exercice défensif sans devenir un incident suisse vérifié. Demandez si le personnel s'appuie sur le numéro affiché pour autoriser des requêtes sensibles. Testez un rappel indépendant à partir de coordonnées déjà fiables.

L'offre du prestataire du 5 novembre et l'annonce téléphonique du 7 novembre fournissent un contexte proche, extérieur aux dates récentes. Elles ne doivent pas être déplacées dans cette période pour les mettre en avant. Leurs questions de validation restent pertinentes après leurs dates de publication.

4.6 Relier les éléments à une décision attribuée

Les opérations de sécurité devraient conserver un dossier interne de la proposition source et du résultat de validation. Une publication peut justifier une enquête sans justifier une déclaration publique d'incident. Consignez le compte, système, ensemble fournisseur ou processus actuel qui serait touché si l'allégation était authentique.

Les équipes de protection des données doivent distinguer lignes de fichiers et personnes uniques, responsabilité organisationnelle et possession de données. Un prestataire peut détenir des informations sur un client sans accéder à ses systèmes de production. Établissez les rôles de responsable du traitement et de sous-traitant à partir de la relation réelle.

Les gestionnaires fournisseurs doivent conserver l'inventaire des informations partagées avec chaque prestataire. Il doit inclure consignes opérationnelles et données d'assistance, en plus des dossiers clients évidents. Cet inventaire permet de comparer les champs annoncés aux flux métier autorisés lors d'une enquête.

La communication doit distinguer l'allégation d'un acteur, les constatations de l'organisation et les questions ouvertes. Répétez seulement les détails nécessaires à une action protectrice. Reproduire des champs sensibles ou des affirmations spectaculaires peut accroître l'incertitude sans aider le lecteur.

POINTS À RETENIR

01

Traitez offre, réponse, demande d'achat et incident confirmé comme des types d'éléments distincts

02

Validez l'âge, la propriété et la pertinence actuelle des informations annoncées avant une action perturbatrice

03

Incluez sécurité physique et responsables fournisseurs lorsque des consignes opérationnelles peuvent être concernées

CHAPITRE 05

Exemples de ciblage par secteur

05

CE CHAPITRE RÉPOND À LA QUESTION

Comment les incidents confirmés modifient-ils les priorités de contrôle des secteurs ?

97 000

enregistrements de permis, sans compter les personnes

5.1 Lire les cas avec leurs limites 41

5.2 Les campagnes relient des secteurs autrement distincts 50

5.3 Activité récente : 9–22 novembre 51

5.4 Autres rapports publics et qualifications plus étroites 52

5.5 Autres incidents cantonaux et campagnes de fraude 53

CHAPITRE 05

Exemples de ciblage par secteur

EN BREF

Les cas suisses confirmés relient vol d'informations, perturbation de services et fraude ultérieure. Une base cantonale de permis, un fournisseur de logiciels de prévoyance et un prestataire énergétique illustrent différentes dépendances. Les cas de santé et de médias montrent pourquoi données touchées et conséquences opérationnelles exigent des descriptions séparées. Les avertissements récents couvrent aussi les commandes frigorifiques. Attribuez chaque réponse au responsable de service, puis vérifiez systèmes, données et preuves de reprise.

5.1 Lire les cas avec leurs limites

Un incident fournisseur et une intrusion dans le système client sont des événements différents. Des données d'une organisation peuvent être touchées chez un prestataire alors que ses systèmes de production continuent. Le service peut aussi être rétabli avant la résolution des conséquences du vol. Ces distinctions déterminent les responsables, messages et critères de réalisation du plan d'incident.

Les cas sont sélectionnés pour leur valeur décisionnelle. Ils ne classent pas les secteurs et ne recensent pas toutes les intrusions suisses. Les dates identifient l'incident ou sa mise à jour publique selon l'étiquette. Les totaux restent rattachés à leur population d'origine. Les annonces publiques ne fournissent pas au rapport d'accès forensique chez les victimes.

Le tableau distingue les principales questions de contrôle avant le détail des fiches.

Secteur	Récit observé	Limite	Première décision
Services cantonaux	Vol de données d'une base de permis	Une personne peut figurer plusieurs fois	Protéger les demandeurs et contacts employeurs
Santé	Rançongiciel interrompant l'accès aux informations d'imagerie	Vol médical non résolu	Tester solutions cliniques alternatives et récupération
Prévoyance	Vol chez un fournisseur déclenchant des enquêtes	L'incident fournisseur ne prouve pas une intrusion en production	Établir l'inventaire des données transférées
Médias	Coordonnées historiques du personnel touchées	Aucune preuve rapportée d'exposition des sources ou recherches	Soutenir le personnel et examiner la conservation
Énergie	Adresses et informations de compteurs volées chez un prestataire	Systèmes et approvisionnement non touchés selon l'entreprise	Rapprocher les ensembles de données du prestataire
Commerce et installations	Paramètres frigorifiques manipulés	Le récit public n'établit aucun acteur nommé	Vérifier températures et alarmes indépendantes

CAS F

F

Permis cantonaux et risque ultérieur d'usurpation (001)

Administration publique

Communication officielle ; enregistrements distincts des personnes

RÉCIT	Bâle-Campagne a confirmé le 20 novembre 2026 un vol dans sa base de permis frontaliers. L'annonce identifiait 97 000 enregistrements, comprenant des informations personnelles et coordonnées d'employeurs. [S17]
CHRONOLOGIE	Une mise à jour du 18 novembre décrivait des effets sur environ 20 applications. La déclaration du 20 novembre confirmait le vol. Le système de permis fonctionnait depuis le 28 novembre 2016. [S47][S17]
ÉTABLI	Le canton citait noms, adresses, dates de naissance, professions et identifiants du système migratoire. La plateforme concernée a été mise hors ligne. Les demandes restaient possibles par d'autres moyens. [S16][S17]
LIMITES	Le canton distingue explicitement enregistrements et personnes. Renouvellements, changements d'adresse et d'emploi peuvent produire des répétitions. La FAQ ne confirme pas le vol des pièces d'identité ou contrats de travail téléversés. [S16]
AUTRES EXPLICATIONS	Les entrées historiques peuvent expliquer une partie du volume. Le total ne peut devenir un nombre de titulaires actuels, de personnes uniques ou de victimes confirmées de fraude d'identité. [S16]
RÉPONSE	Les services publics et RH des employeurs doivent identifier les processus touchés, conserver l'avertissement officiel et vérifier indépendamment les demandes inhabituelles. Des renseignements personnels exacts ne remplacent pas l'authentification.

En définitive

Validez les processus des demandeurs et employeurs, puis utilisez des contacts fiables.

La conclusion justifiable est un vol confirmé lié à une base, avec un périmètre individuel non résolu. Elle ne compte pas 97 000 personnes. La protection immédiate inclut les employeurs, car leurs contacts administratifs figurent aussi dans les informations concernées. [S16]

CAS G

G Continuité radiologique et questions distinctes sur le vol (O02)

Santé

Rançongiciel rapporté ; vol médical non résolu

RÉCIT	Groupe 3R indique qu'une attaque par rançongiciel a eu lieu le 30 avril 2026. Il rapporte chiffrement et vol d'informations administratives, dont des informations sur les employés actuels et anciens. [S18]
CHRONOLOGIE	Les soins ont été particulièrement affectés les 1 et 2 mai. L'exploitant indique une infrastructure reconstruite dans les centres dès le 26 juin. Sa page publique comporte une mise à jour du 22 septembre. [S18]
ÉTABLI	Les résultats d'examens ont été chiffrés, affectant leur disponibilité. Les centres seraient restés ouverts selon l'exploitant, avec certains examens retardés, reprogrammés ou réorientés. Les principaux systèmes et la téléradiologie ont ensuite été rétablis. [S18]
LIMITES	L'exploitant ne pouvait établir avec certitude si des informations médicales de patients avaient aussi été volées. L'absence de publication confirmée de ces fichiers ne résout pas cette question. [S18][S19]
AUTRES EXPLICATIONS	Rétablissement du service et confidentialité nécessitent des clôtures distinctes. L'exploitant décrit l'événement 2026 comme sans rapport avec celui de 2025. L'ancienne attaque ne peut être recomptée comme un nouveau cas 2026. [S18]
RÉPONSE	Les opérations cliniques doivent tester l'accès aux résultats, les orientations alternatives et les confirmations de rendez-vous. Sécurité et protection des données doivent évaluer séparément le vol et les fraudes ultérieures visant les patients.

En définitive

Testez le parcours clinique et évaluez la confidentialité séparément de la restauration.

ICTjournal rapporte que l'exploitant attribuait l'attaque à Akira d'après ses partenaires spécialisés. C'est l'attribution de l'exploitant rapportée par le média. Le rapport ne dispose d'aucune preuve technique indépendante reliant un acteur à l'incident. [S19]

Pour les responsables de santé, un test de restauration réussi doit couvrir tout le parcours clinique. Restaurer un serveur ne démontre pas la récupération des images, l'interprétation des examens et la communication avec les cabinets prescripteurs.

CAS H

H ■ Données d'un fournisseur de prévoyance et périmètre d'enquête (O03)

Prévoyance

Incident fournisseur ; enquête en cours

RÉCIT	Publica a confirmé une fuite après une attaque identifiée fin septembre par un fournisseur externe de logiciels. Le fournisseur a informé Publica, d'autres clients et les autorités fédérales compétentes. [S21]
CHRONOLOGIE	Publica a communiqué initialement aux assurés le 8 octobre. Le PFPDT a reçu l'annonce du fournisseur ce jour-là. Il a commencé ses clarifications concernant Publica le 14 octobre et ouvert une enquête fournisseur le 22 octobre. [S21][S15]
ÉTABLI	Le PFPDT indique que des données de plusieurs institutions de prévoyance ont été emportées. Son enquête examine les informations personnelles fournies, le cadre juridique des transferts et l'étendue des données perdues. [S15]
LIMITES	Une fuite confirmée chez un fournisseur n'identifie pas chaque personne, chaque champ ou l'état opérationnel de tous les systèmes clients. L'enquête était en cours dans l'annonce citée. [S15]
AUTRES EXPLICATIONS	Un jeu de travail détenu par un fournisseur et une base de prévoyance de production ont des rôles différents. Le récit public ne doit pas devenir une affirmation infondée d'accès à cette dernière.
RÉPONSE	Les administrateurs de prévoyance doivent rapprocher les ensembles conservés par le fournisseur des finalités contractuelles et durées de conservation. Les services aux assurés doivent vérifier indépendamment l'identité des appelants connaissant déjà des détails personnels ou financiers.

En définitive

Rapprochez les informations du fournisseur des finalités contractuelles et de la protection des assurés.

Le cas crée deux chantiers distincts. Le premier établit les informations détenues et volées. Le second protège les assurés contre des démarches convaincantes réutilisant ces informations. Le lien entre ces chantiers doit être explicite dans les communications clients.

Cybercrimepolice avertit aussi de démarches d'investissement après une fuite chez un prestataire de prévoyance. Il évoque l'usage possible d'informations salariales et de retraite. Cet avertissement justifie la préparation antifraude ; il ne vérifie pas tous les champs volés chez ce fournisseur. [S45]

Le 19 novembre, Publica annonçait un examen externe des achats, traitements de données personnelles, contrôles de sécurité et gouvernance. L'environnement de test du fournisseur était concerné, les systèmes de production de Publica étant déclarés intacts. Les investigations techniques sur les personnes et données touchées restaient inachevées. [S55]

CAS I

Données historiques du personnel des médias et limites du récit élargi (O04)

Médias

Données historiques du personnel rapportées

RÉCIT	SRG a signalé le 28 septembre un cyberincident concernant des données de contact et d'organisation de 2020, relatives à environ 340 employés actuels et anciens de SRF. [S20]
CHRONOLOGIE	SRG dit avoir désactivé l'accès concerné, renforcé la sécurité, annoncé le cas aux autorités et informé les personnes. L'enquête était en cours lors de l'annonce. [S20]
ÉTABLI	Les informations comprenaient noms, fonctions et coordonnées professionnelles, avec certaines coordonnées privées. SRG décrivait la population touchée et soutenait les personnes concernées. [S20]
LIMITES	SRG ne rapportait aucun indice concernant mots de passe, données financières, sources journalistiques, recherches ou contenus des communications. Aucun indice de publication ou d'usage abusif n'était rapporté à ce stade. [S20]
AUTRES EXPLICATIONS	Les données historiques du personnel peuvent conserver une valeur d'ingénierie sociale. Leur présence ne prouve aucune ingérence dans les reportages, décisions éditoriales ou opérations de diffusion.
RÉPONSE	Sécurité et RH doivent examiner pourquoi des ensembles historiques de contacts restent accessibles. Le soutien au personnel doit couvrir usurpations et démarches suspectes sans présenter des conséquences non vérifiées comme des dommages établis.

En définitive

Examinez conservation et accès tout en protégeant le personnel contre l'usurpation.

La leçon concerne la conservation des informations et la gouvernance des accès. Le rôle médiatique d'une organisation ne justifie pas l'attribution d'un motif politique. Le récit cité n'en fournit aucune base. Le rapport sépare donc la catégorie touchée et la cause non résolue. [S20]

CAS J

J ■ Données de prestataire sans incident d'approvisionnement énergétique (O05)

Énergie et services collectifs

Données de prestataire ; systèmes déclarés non touchés

RÉCIT	IWB annonçait le 15 juillet le vol d'environ 40 000 enregistrements d'adresses détenus par un prestataire. Ils comprenaient des détails techniques sur les compteurs d'énergie. [S40]
CHRONOLOGIE	Le prestataire a informé IWB après détection. IWB a vérifié les accès, limité les échanges avec lui et écrit aux clients concernés. [S40]
ÉTABLI	IWB identifiait noms, adresses, numéros de compteurs et caractéristiques d'installation. L'entreprise déclarait ses systèmes et la sécurité d'approvisionnement non affectés. [S40]
LIMITES	Selon IWB, l'ensemble volé ne contenait ni courriels, ni téléphones, ni consommations, ni données bancaires ou de paiement. Aucun indice d'usage abusif n'était rapporté à ce stade. [S40]
AUTRES EXPLICATIONS	Des données associées à une entreprise énergétique ne prouvent pas un accès aux commandes opérationnelles. Adresses et compteurs ne doivent pas être décrits comme un profil financier client complet.
RÉPONSE	Les gestionnaires fournisseurs doivent valider l'inventaire partagé avec les prestataires. Le service client doit se préparer aux démarches citant une adresse ou un compteur réel pour exiger paiement urgent ou informations supplémentaires.

En définitive

Rapprochez les informations du prestataire et préparez le service client aux demandes convaincantes.

IWB rapportait que l'autorité cantonale de protection des données estimait faible le risque d'usage abusif. Cette évaluation concerne les informations et circonstances décrites. Elle ne doit pas devenir une déclaration générale d'innocuité du vol chez les prestataires. [S40]

CAS K

K ■ Commandes frigorifiques et vérification indépendante du processus physique (O06)

Commerce et installations

Avertissement officiel ; acteur non attribué

RÉCIT	L'OFCS avertissait le 10 novembre d'attaques contre des commandes frigorifiques en Suisse. Un avis policier du 12 novembre décrit des réglages manipu-

lés chez une entreprise suisse, avec écarts importants de température et fermeture temporaire d'une succursale. [S53][S41]

CHRONOLOGIE	Ces avis appartiennent à la période récente. Ils traitent d'attaques connues dans les semaines précédentes. Ils ne fournissent pas de date vérifiée du premier accès à l'entreprise. [S53][S41]
ÉTABLI	L'avis policier décrit la modification possible des températures, cycles de dégivrage et alarmes par des interfaces de gestion insuffisamment protégées. Il recommande de mesurer les températures réelles avec un instrument indépendant. [S41]
LIMITES	Les récits disponibles n'établissent ni acteur nommé ni motif politique. L'avertissement technique couvre plusieurs familles de produits, sans identifier le système d'une victime particulière. [S53]
AUTRES EXPLICATIONS	Une alarme silencieuse ne prouve pas un processus sain si ses réglages peuvent être modifiés. Panne et modifications non autorisées exigent des enquêtes différentes, mais toutes deux nécessitent des vérifications indépendantes de sécurité.
RÉPONSE	Installations, frigoriste et informatique doivent examiner ensemble accès distants, logiciels maintenus et transmission des alarmes. Protégez la maintenance distante nécessaire et confirmez les températures réelles avant la reprise normale.

En définitive

Vérifiez indépendamment la température physique et examinez les accès de gestion distante.

Ce cas limite aussi l'interprétation des anciennes évaluations nationales. L'OFCS ne rapportait aucun cybersabotage ciblé connu en Suisse dans son bilan semestriel. Un incident industriel ultérieur doit être examiné selon ses propres faits, sans être réétiqueté en sabotage étatique. [S5][S41]

L

CAS L

Accès collaboratifs fédéraux et comptes touchés (O07)

Administration publique

Récit officiel · environ 200 comptes

RÉCIT	L'office fédéral informatique annonçait le 4 août qu'environ 200 comptes utilisateurs et techniques avaient été touchés par une attaque contre ses serveurs SharePoint. [S54]
CHRONOLOGIE	Des spécialistes avaient détecté une activité inhabituelle le 28 juillet. L'analyse identifiait des identifiants touchés le 31 juillet. L'office réinitialisait les mots de passe, bloquait l'accès Internet externe et lançait la reconstruction. [S54]

ÉTABLI	Le récit distingue identifiants touchés et autres informations. L'analyse disponible à publication ne montrait aucun indice de vol supplémentaire. Les utilisateurs internes conservaient l'accès documentaire et des moyens alternatifs de partage. [S54]
LIMITES	L'absence d'indices déclarée n'est pas une conclusion forensique achevée. L'avis ne nomme aucun acteur. Il ne justifie ni motif attribué ni extension de la population au-delà des comptes décrits. [S54]
RÉPONSE	Les responsables collaboratifs doivent tester la révocation d'identifiants et l'échange documentaire alternatif. Séparez l'autorité de réouverture externe des preuves nécessaires à la clôture de l'enquête sur le vol.

En définitive

Validez comptes et services touchés sans déduire de population élargie.

M

CAS M

Tickets scolaires et usurpation ciblée de l'assistance (O08)

Formation

Communication officielle ; contacts scolaires

RÉCIT	Vaud rapportait une copie non autorisée de noms et adresses scolaires concernant environ 3500 enseignants et 38000 élèves. Les contenus des demandes d'assistance avaient aussi été copiés. [S59]
CHRONOLOGIE	Le canton détectait l'accès non autorisé le 26 octobre. Il déconnectait la plateforme, la sécurisait avec son centre opérationnel de sécurité et informait directement les utilisateurs. [S59]
ÉTABLI	Le service traitait les demandes informatiques de la formation postobligatoire. Le canton précisait que les mots de passe n'y étaient pas stockés. Les notes et dossiers scolaires n'étaient pas touchés. [S59]
LIMITES	Le texte d'un ticket et une base scolaire sont des populations différentes. Le cas n'établit pas l'obtention de tous les mots de passe ou dossiers scolaires. [S59]
RÉPONSE	L'informatique scolaire doit avertir des messages usurpant l'école ou l'assistance. Exigez des demandes vérifiées et examinez la conservation de pièces jointes ou textes libres au-delà des besoins opérationnels.

En définitive

Protégez les identités scolaires touchées et vérifiez les contacts inhabituels par des voies fiables.

CAS N

N ■ Formation d'adultes et évaluation évolutive des données touchées (O09)

Formation

Incident officiel : périmètre révisé ensuite

RÉCIT	Ifage indique qu'une attaque des 11–12 avril a conduit à un vol, détecté le 13 avril. Son avis ultérieur explique que la publication du 23 juillet établissait aussi l'implication des données d'apprenants et clients. [S58]
ÉTABLI	L'institution identifie données administratives des cours, coordonnées et documents d'examens. Certains fichiers incluaient pièces d'identité, candidatures ou justificatifs d'absence. Elle précise que la continuité opérationnelle a été maintenue. [S58]
LIMITES	L'avis ne fournit aucun total vérifié de personnes concernées. Une précision ultérieure élargit le périmètre connu d'un incident, sans créer une seconde intrusion. [S58]
AUTRES EXPLICATIONS	Une première annonce peut refléter correctement une enquête incomplète. Il faut distinguer cette connaissance évolutive d'une nouvelle attaque ou d'un accès persistant vérifié.
RÉPONSE	Formation et protection des données doivent tenir un registre versionné des impacts. Mettez à jour les communications directes lorsque de nouvelles catégories sont établies, en conservant date et base de l'évaluation antérieure.

En définitive

Gardez l'évaluation révisée des données distincte du rétablissement antérieur du service.

CAS O

O ■ Formulaires universitaires pendant la période récente (O10)

Formation

Communication officielle ; formulaires en ligne

RÉCIT	USI annonçait le 19 novembre un accès non autorisé aux informations d'un système vulnérable de formulaires entre le 9 et le 17 novembre. [S80]
ÉTABLI	L'application servait à certaines candidatures, demandes de bourses et enquêtes. Réponses et pièces jointes étaient sur le serveur concerné. L'université le sécurisait et informait les autorités et personnes potentiellement touchées. [S80]

LIMITES	USI indiquait encore établir le périmètre, la sensibilité et les risques. L'annonce ne donnait aucun total vérifié de personnes et ne prouvait pas la copie de chaque pièce jointe. [S80]
AUTRES EXPLICATIONS	Les formulaires collectent des informations différentes. Candidats à l'emploi, aux bourses et participants aux enquêtes ne doivent pas constituer une population uniforme de risque.
RÉPONSE	Les responsables applicatifs doivent identifier finalités et durées de conservation des formulaires touchés. Demandez aux destinataires de vérifier les demandes inattendues de documents, coordonnées bancaires et paiements par un canal universitaire établi.

En définitive

Identifiez les formulaires touchés, conservez l'avis et vérifiez indépendamment les demandes ultérieures.

5.2 Les campagnes relient des secteurs autrement distincts

Plusieurs avertissements officiels décrivent un mécanisme commun plutôt qu'une victime nommée. Le client d'un fournisseur, un employé et un ménage peuvent rencontrer des étapes de fraude liées. Cette séquence n'établit pas qu'elles appartiennent toutes au même opérateur.

Le tableau conserve l'unité de la source et identifie une réponse proportionnée.

Date d'avis	Récit de campagne	Incertitude restante	Décision de défense
2026-02-03	Un partage SharePoint authentique menait au phishing en temps réel [S24]	L'avis ne compte pas toutes les organisations touchées	Examiner tout le parcours des liens et l'exposition des sessions
2026-02-10	Le bombardement d'abonnements masquait des messages importants de comptes [S25]	Une boîte saturée ne prouve pas un paiement frauduleux	Rechercher modifications de comptes, commandes et paiements
2026-02-24	Des leurres ClickFix incitaient à exécuter des commandes nuisibles [S26]	L'action utilisateur ne révèle pas tout le chemin d'intrusion	Orienter les fausses réparations vers l'assistance et examiner les terminaux
2026-04-14	De faux banquiers demandaient un logiciel de télémaintenance [S27]	Une marque bancaire citée ne prouve pas une intrusion bancaire	Vérifier indépendamment les appels et restreindre l'assistance distante non sollicitée
2026-05-05	Un phishing de colis était suivi d'un appel de fausse banque [S28]	Ampleur et opérateur non établis	Expliquer aux clients ce qu'autorise réellement une confirmation de paiement

Date d'avis	Récit de campagne	Incertitude restante	Décision de défense
2026-06-09	Des demandeurs d'emploi subissaient phishing d'entretien, demandes de paiement et leurres malveillants [S30]	L'avis décrit plusieurs stratagèmes	Séparer recrutement et paiements
2026-09-01	Un site de livraison alimentaire servait au vol tenté de données de paiement [S32]	La source n'identifie pas chaque transaction touchée	Surveiller changements de pages de paiement et contenus tiers
2026-10-20	Des leurres de réservation visaient paiements mobiles et accès bancaires [S34]	Les détails de réservation ne prouvent pas toutes les causes initiales	Confirmer les demandes inhabituelles auprès du prestataire réservé

5.3 Activité récente : 9–22 novembre

Des détails personnels exacts ne prouvent plus la fiabilité d'une demande. L'avis OFCS du 17 novembre relie une fuite antérieure chez un prestataire domestique à du phishing ciblé ultérieur. Les messages réutilisaient noms, adresses et numéros d'assurance sociale. L'avis décrit aussi du phishing prétextant une mise à jour PHP. [S14]

L'avis policier de la même semaine décrit des messages de réservation contenant de vrais détails d'hébergement et références. Les attaquants demandaient une prétendue confirmation puis des données de carte. Le rapport conserve le rôle du prestataire, son admissibilité à être nommé n'étant pas pleinement établie. [S43]

L'avertissement policier du 18 novembre ajoute une étape de paiement physique. Des appelants usurpaient le personnel bancaire et utilisaient une fausse lettre de banque centrale pour demander des espèces destinées à un prétendu compte de protection. L'autorité revendiquée fait partie de la fraude, sans prouver une implication de la banque centrale. [S44]

La mise à jour de Bâle-Campagne du 20 novembre rend immédiate la question du passage des données à la fraude. Les RH doivent prévoir des démarches citant des détails réels d'emploi ou de permis. L'avis officiel justifie une vigilance accrue, sans établir que chaque personne concernée a déjà reçu un message frauduleux. [S16][S17]

L'avis USI du 19 novembre ajoute formulaires et pièces jointes aux priorités immédiates. Celui de Publica le même jour concerne l'examen externe de gouvernance de son incident fournisseur existant. Ce sont des évolutions différentes : nouvel incident universitaire divulgué et réponse ultérieure à un événement antérieur de prévoyance. [S80][S55]

Ces mises à jour justifient un exercice pratique en novembre. Présentez au service client et à l'assistance une demande inattendue comportant des détails personnels exacts. Exigez vérification indépendante, conservation du message et consignation de la décision. Mesurez le respect du processus fiable malgré la crédibilité des informations.

5.4 Autres rapports publics et qualifications plus étroites

Ces éléments élargissent la couverture sectorielle sans adopter de récit d'acteur non vérifié. Sans confirmation publique directe conservée, l'organisation reste décrite par son rôle. La publication citée est la source du récit organisationnel rapporté.

Date	Rôle	Récit rapporté	Qualification
2026-01-23	Opérateur radio et événementiel	Base événementielle externe touchée ; mots de passe et paiements exclus du périmètre rapporté [S56]	Exemple d'exposition de données fournisseur
2026-03-04	Fournisseur de logiciels métier	Incident reconnu avec effets opérationnels limités ; volume de données annoncé séparément restant une affirmation [S50]	Affirmation et impact séparés
2026-03-25	Prestataire d'ingénierie	Incident de février suivi d'une déconnexion préventive et d'une restauration rapportée [S48]	Vérifier les factures fournisseurs inattendues
2026-04-14	Fabricant de produits médicaux	Ancien système interne et documents anciens identifiés dans le récit de l'entreprise rapporté [S49]	Exemple de conservation sur système ancien
2026-08-26	École de commerce	Incident externe affectant étudiants et anciens élèves ; opérations locales poursuivies selon l'école [S57]	Fournisseur et systèmes locaux distincts
2026-07-09	Prestataire d'hébergement et de soins	Rançongiciel perturbant les systèmes ; reconstruction partielle et soins poursuivis en octobre [S81]	Tester communications prolongées et soins alternatifs
2026-03-14	Administration communale	Chiffrement partiel puis restauration ; aucun indice de vol selon la commune [S86]	Séparer restauration et conclusions sur le vol
2026-07	Fabricant industriel	Revue cantonale décrivant accès à une plateforme fournisseur et demande d'extorsion distincte [S84]	Confirmer le périmètre des plateformes partagées
2026-07	Services fiduciaires	Revue cantonale décrivant des dossiers clients publiés après un incident [S84]	Inventorier documents fiscaux et clients chez les conseillers

Date	Rôle	Récit rapporté	Qualification
2026-09	Laboratoire partenaire d'hôpital	Revue cantonale décrivant des informations patients touchées dans un laboratoire externe [S85]	Rapprocher transferts de laboratoire et contacts patients
2026-10-26	Plateforme d'administration sportive	Fédération confirmant accès non autorisé puis offre sur forum ; mots de passe non touchés [S88]	Examiner autorisations et avertir les participants
2026-10-31	Plateforme de licences sportives	La fédération a confirmé un incident touchant des données personnelles ; son périmètre complet restait à établir. [S87]	Ne pas transformer les lignes annoncées en personnes
2026-11-16	Site de streaming	Chercheur signalant des scripts tiers malveillants sur un service suisse [S89]	Examiner dépendances navigateur et avis fournisseurs

La mise à jour d'octobre du prestataire de soins supposait toujours une fuite, sans en établir l'étendue. Elle assurait le maintien des soins de base, du soutien médical et de la sécurité des résidents. Le retour prévu à la normale fin novembre était une prévision, pas une date confirmée. [S81]

Les avis officiels distinguent aussi défense et intrusion. Une autorité publique a signalé des restrictions temporaires de services lors de la correction de vulnérabilités PHP en octobre, sans attaque correspondante constatée. L'avertissement du PFPDT en avril concernait l'usurpation du régulateur, sans accès à ses systèmes. [S83][S82]

Ces exemples ne doivent pas devenir de nouvelles fiches dans les totaux de cas. Ce sont des mentions d'incidents. Cette différence est un choix de présentation, sans implication d'un impact métier inférieur.

5.5 Autres incidents cantonaux et campagnes de fraude

Séparez accès non autorisés et restrictions préventives. Une autorité cantonale rapportait un incident SharePoint le 5 août. L'analyse préliminaire ne révélait ni comptes touchés ni vol. Une mise à jour du soir devait interrompre temporairement le site public. Les autres applications restaient disponibles. L'annonce décrit un incident distinct du cas collaboratif fédéral. [S90]

Les informations publiques peuvent aussi permettre des fraudes convaincantes. Un avis conjoint du 28 août décrivait la collecte automatisée de données publiques de détenteurs de véhicules dans cinq cantons. Les entrées protégées n'étaient pas touchées. L'avis décrivait aussi des tentatives d'extorsion et des demandes de paiement susceptibles de réutiliser ces informations. Il ne prouve pas un vol de données protégées. [S91]

Les avis policiers ajoutent des éléments locaux au schéma annuel d'usurpation. Ils concernent des périodes et populations différentes. Leurs nombres ne doivent pas former un total national d'incidents ou de pertes.

Avis	Récit policier	Limite de périmètre	Action
2026-01	Vaud recensait 24 cas de faux banquiers ou policiers la semaine du 12 janvier, dont 12 tentatives [S92]	Une semaine cantonale	Former le personnel en contact client aux demandes urgentes d'espèces
2026-02-10	Saint-Gall décrivait une fraude d'accès distant causant une perte individuelle supérieure à CHF 500 000 fin janvier [S93]	Perte d'une personne rapportée	Vérifier l'assistance non sollicitée avant l'accès distant
2026-04-24	Le Tessin décrivait une tentative d'urgence familiale interrompue après un signalement rapide [S94]	Tentative rapportée par la police, sans perte accomplie	Établir un canal fiable de vérification familiale
2026-06-10	Berne avertissait de fraudes d'accès distant avec pertes importantes [S95]	Période de novembre 2025 à avril 2026	Ne pas attribuer tout le montant à 2026
2026-09-24	Deux coursiers présumés déclaraient avoir accepté des offres d'emploi en ligne [S96]	Leur récit n'identifie pas tout un réseau	Examiner les collectes rémunérées d'enveloppes
2026-10-13	Des messages menaient à des appels puis à la collecte de cartes à puce intacte [S97]	Plusieurs enquêtes et observations	Faire remonter les demandes de collecte de cartes
2026-10-29	Neuchâtel rapportait alors 160 cas établis en 2026, pertes estimées autour de CHF 950 000 [S98]	Signalements cantonaux jusqu'à l'avis	Conserver la période dans les notes à la direction
2026-11-10	Le Valais décrivait environ 40 signalements depuis mi-octobre, tentatives et fraudes accomplies [S99]	Une tentative signalée n'est pas une perte accomplie	Consigner le résultat en plus de la démarche
2026-11-19	Zoug décrivait deux enquêtes de coursiers et une intervention déclenchée par du personnel bancaire [S100]	Deux cas indépendants, enquêtes en cours	Maintenir une escalade pour les retraits inhabituels

Ces avis justifient un contrôle commun aux banques, services clients et familles. Un appelant convaincant peut combiner institution familière, détails réels et urgence. Un coursier ajoute ensuite une étape physique. Vérifiez par un canal connu avant de transférer de l'argent, remettre une carte ou autoriser l'accès distant. [S92][S93][S97][S100]

Le récit de Schaffhouse relie aussi l'examen d'offres d'emploi à la prévention. Il n'établit pas que chaque coursier comprend le but de la collecte. Employeurs, plateformes et candidats doivent examiner les tâches anormalement faciles impliquant espèces ou enveloppes scellées, sans supposer un acteur unique. [S96]

Les avis de novembre renforcent l'analyse récente sans établir une croissance nationale. Les totaux locaux dépendent de leurs périodes et populations déclarées. Un avertissement ou une arrestation témoigne utilement d'un mécanisme actif, sans mesurer la prévalence nationale. [S99][S100]

POINTS À RETENIR

01

Décidez séparément du rétablissement des services et de l'évaluation du vol

02

Distinguez enregistrements, personnes et organisations

03

Vérifiez les demandes inattendues même si l'expéditeur connaît de véritables détails personnels

CHAPITRE 06

Hacktivisme et DDoS

06

CE CHAPITRE RÉPOND À LA QUESTION

Que permettent d'établir les incidents de disponibilité sur l'impact, l'attribution et le motif ?

40 minutes

interruption Internet rapportée chez Salt

6.1 Le récit officiel 2026 57

6.2 Affirmation et informations rapportées 57

6.3 Comparaison historique datée : le sommet 2024 58

6.4 Chronologie et décisions de réponse 58

6.5 Disponibilité de la messagerie et canal d'information indépendant 59

CHAPITRE 06

Hacktivisme et DDoS

EN BREF

Les attaques de disponibilité nécessitent un relevé d'impact distinct de la publicité des acteurs. L'OFCS décrit des perturbations DDoS limitées au premier semestre 2026, avec une interruption télécom notable. Les attaques historiques du sommet restent des exemples de préparation, datés de 2024. Ni rhétorique nationale ni interruption réussie ne prouve un accès interne. Consignez service touché, impact client, attribution de source et preuves de reprise avant l'escalade.

6.1 Le récit officiel 2026

Impact sur la disponibilité et publicité sont des mesures différentes. Dans son bilan semestriel, l'OFCS décrit une activité DDoS restant gérable pour les organisations suisses. Les attaques hacktivistes auraient été pratiquement absentes des grands événements comme le WEF ou les Jeux olympiques d'hiver. Il décrit aussi des tentatives contre le DNS et certains services bancaires sans interruption importante. [S5]

Ces déclarations concernent la période et la visibilité de l'autorité. Elles ne prouvent ni absence de tentatives, ni signalement exhaustif, ni maintien du schéma jusqu'en novembre. Toute annonce ultérieure d'acteur doit donc être évaluée comme un nouvel élément.

Le rapport identifie Salt comme l'impact DDoS largement perceptible de la période. Netzwoche rapporte environ 40 minutes sans Internet fixe le 15 mai. Le réseau mobile continuait à fonctionner. Le média indiquait que l'acteur, le motif et une éventuelle rançon restaient inconnus. [S5][S22]

Ne transformez pas une interruption télécom en affirmation infondée de vol client. Un site public interrompu ne prouve pas davantage une intrusion dans le réseau interne. La réponse exige des responsables séparés pour disponibilité, analyse d'intrusion et communication client.

6.2 Affirmation et informations rapportées

Le panneau sépare volontairement les mesures. Il conserve une attribution non résolue sans combler la lacune par un nom plausible.

Point	Affirmation d'acteur	Récit officiel	Informations publiques
Impact télécom 2026	Aucune déclaration authentifiée n'établit ici la responsabilité	L'OFCS identifie une interruption DDoS notable chez Salt dans son bilan semestriel [S5]	Environ 40 minutes d'interruption Internet fixe le 15 mai [S22]
Périmètre réseau	Aucune revendication vérifiée n'établit d'accès élargi	Le récit officiel concerne la disponibilité [S5]	Le mobile continuait selon le reportage cité [S22]
Motif	Aucun motif indépendamment étayé	Le bilan national cité n'attribue aucun objectif politique à cet incident [S5]	Identité et motif restaient inconnus dans la publication [S22]
Données internes	Une interruption ne fournit aucune preuve de vol	Le récit de disponibilité cité n'établit aucune telle conclusion [S5]	Le reportage décrit les effets de panne, sans incident interne confirmé [S22]

Le panneau impose une discipline de réponse. Une revendication bruyante peut accompagner un impact limité ; une attaque anonyme peut fortement affecter les clients. Aucun rapport chiffré revendication-impact n'est possible sans mesures du même événement et de la même unité.

6.3 Comparaison historique datée : le sommet 2024

Le Sommet sur la paix en Ukraine s'est tenu les 15–16 juin 2024. Dans son bilan du 20 juin, le NCSC attribuait les DDoS associés à NoName057(16). L'autorité décrivait de faibles perturbations et indiquait que systèmes et données du sommet n'étaient pas menacés. Ces conclusions sont celles du NCSC. [S42]

Le même bilan distingue d'autres incidents des DDoS. Il décrit des tentatives d'intrusion cantonales et du phishing visant des collaborateurs de centrales d'urgence. Les problèmes techniques de diffusion et la panne électrique régio-
nale n'étaient pas cyber. Ces distinctions empêchent d'intégrer des perturbations sans lien au récit d'attaque. [S42]

Cette comparaison ne compte aucun incident 2026. Elle n'établit ni responsabilité dans l'attaque télécom 2026 ni campagne actuelle contre toutes les organisations événementielles. Le rapport ne prend position ni sur le sommet, ni sur les sanctions, relations européennes ou politiques gouvernementales.

La leçon transférable concerne la préparation. Le NCSC décrit un réseau public-privé de suivi de situation, une préparation précoce et une réponse coordonnée. Les organisateurs peuvent en tirer contacts de communication, protection des services publics et méthodes de mesure des perturbations. [S42]

6.4 Chronologie et décisions de réponse

La chronologie distingue contexte historique, date d'incident 2026 et dates de publication ultérieures.

20 juin 2024 **NCSC**
Bilan historique attribuant les DDoS du sommet à NoName057(16), avec faibles perturbations [S42]

15 mai 2026	**Informations publiques** Interruption Internet fixe de Salt décrite ensuite comme un DDoS [S22]
24 août 2026	**OFCS** Bilan semestriel décrivant un impact DDoS gérable et l'interruption télécom [S5]
18 nov. 2026	**Administration cantonale** Bâle-Campagne déclarait les systèmes d'urgence et de secours opérationnels pendant son incident informatique distinct [S47]

La mise à jour cantonale de novembre figure ici pour la communication, sans attribution DDoS. Une alerte précoce sur une perturbation possible ne doit pas devenir une panne observée des secours. Le canton précisait que les systèmes concernés n'avaient jamais été touchés. [S47]

L'escalade opérationnelle doit suivre la dégradation observée et une conséquence métier documentée. Conservez dates de début et de reprise, fonction touchée et mesures propres à l'organisation. Une capture d'écran tierce fournit une piste, sans relevé complet d'impact.

La communication doit distinguer site public, authentification client, réseau de communication et systèmes internes. Les mises à jour doivent porter sur les fonctions utilisables et alternatives disponibles. Évitez slogans d'acteurs et motifs politiques affirmés comme des faits.

Les responsables de services doivent exercer le moment où une protection réduit les fonctions. Convenez de l'autorisation, de l'explication et de la validation de reprise. Le dossier doit distinguer confinement préventif et dommages causés par un attaquant.

6.5 Disponibilité de la messagerie et canal d'information indépendant

Le récit publié par Threema le 14 août 2026 décrit des perturbations par DDoS les 11–12 août. L'entreprise a signalé une indisponibilité entre 19:30 et 23:30 CEST le mardi, puis des interruptions intermittentes le mercredi matin. Elle a annoncé le rétablissement du fonctionnement normal à 12:23 le mercredi. L'événement relève du second semestre 2026. [S101]

L'entreprise a décrit des attaques touchant son service et un partenaire de colocation. Elle n'a pas pu établir si Threema était la cible principale ou l'une de plusieurs cibles. Selon l'entreprise, les clients utilisant Threema OnPrem sur leur propre infrastructure n'ont pas été touchés. Ce récit d'indisponibilité ne permet ni d'attribuer l'attaque à un acteur étatique ni d'en déduire un accès aux messages internes. [S101][S102]

Un problème technique distinct a d'abord empêché la mise à jour de la page d'état. Threema a temporairement mis cette page hors ligne. Sa mise à jour du 14 août indique qu'une protection DDoS supplémentaire avait été activée. L'entreprise prévoyait aussi un historique des incidents et un flux de notifications indépendant. Ces déclarations datées décrivent sa réponse, sans évaluer l'efficacité actuelle des mesures de protection. [S101]

Pour les responsables de service, ce cas justifie de tester un autre moyen de communication en complément des mesures de protection de la disponibilité. Vérifiez que les clients peuvent distinguer l'indisponibilité du service de celle de sa page d'état. Conservez séparément les horaires d'interruption et de rétablissement de chaque fonction.

POINTS À RETENIR

01

Attribuez la responsabilité d'un acteur uniquement à la source qui l'établit

02

Excluez le sommet 2024 des totaux d'incidents 2026

03

Mesurez service touché et reprise avant d'amplifier le récit d'un acteur

CHAPITRE 07

Acteurs de la menace et relations étayées

07

CE CHAPITRE RÉPOND À LA QUESTION

Quelles descriptions d'acteurs aident la défense sans exagérer l'attribution ?

41

noms de groupes dans l'instantané suisse des rançongiciels

7.1 Les marques décrivent des inscriptions, sans historique complet d'intrusion 62
7.2 Contexte régional sans classement des pays 65
7.3 Pseudonymes et relations dans les publications retenues 65
7.4 Activité liée à des États selon le SRC 67
7.5 Matrice de techniques pour planifier les contrôles 68
7.6 Préparation aux correctifs : avertissement PHP d'octobre 69
7.7 Acteurs au discours politique 69
7.8 Ce qui renforcerait une évaluation d'acteur 70
7.9 Altérations temporaires des mises à jour et éléments de preuve rétrospectifs 70

CHAPITRE 07

Acteurs de la menace et relations étayées

EN BREF

Les éléments offrent des vues distinctes : marques de rançongiciels, pseudonymes proposant des données, revendications politiques de disponibilité et évaluations officielles d'espionnage. Ils ne forment pas un réseau prouvé. AKIRA détient le plus d'inscriptions suisses dans cet instantané ; les autres marques restent majoritaires ensemble. Les attributions nationales et étatiques restent celles de l'autorité citée. Utilisez les informations d'acteurs pour choisir les questions d'enquête et scénarios de reprise.

7.1 Les marques décrivent des inscriptions, sans historique complet d'intrusion

Ransompedia recense 122 inscriptions suisses sous 41 noms de groupes pendant la période. AKIRA en représente 13 ; The Gentlemen (inscrit sous Thegentlemen dans l'instantané brut) et Qilin 9 chacune. Ces trois noms regroupent 31 inscriptions, soit 25.4% du total suisse. Les 91 restantes représentent 74.6% [S2].

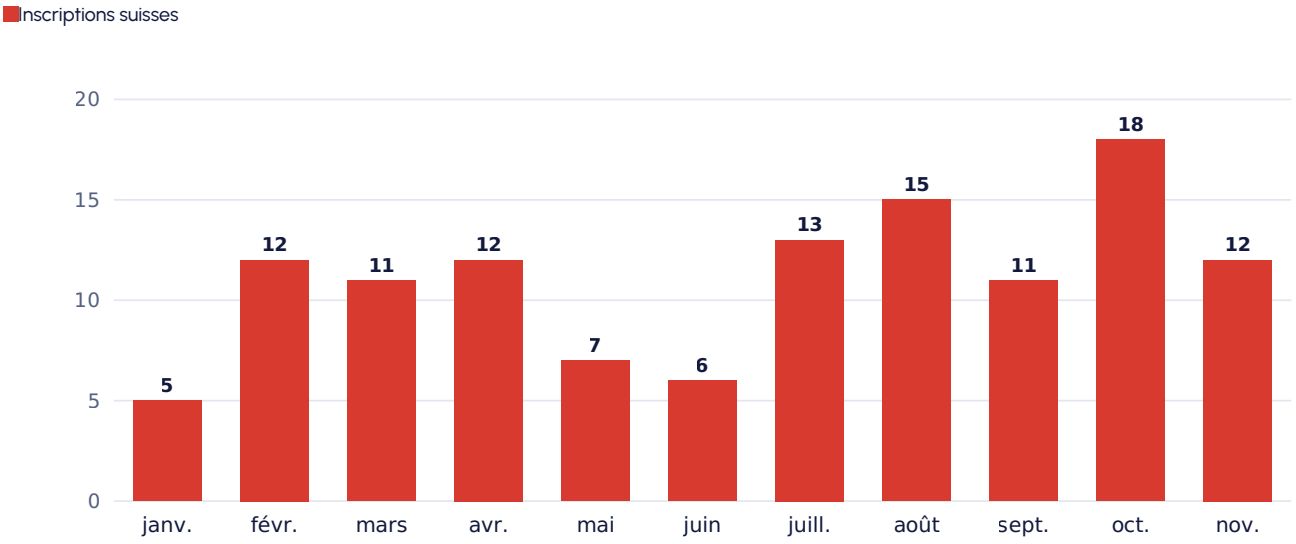
Cette répartition plaide contre une continuité conçue autour d'une seule marque. Les noms peuvent changer, les organisations apparaître plusieurs fois et les logiciels rester inconnus malgré une revendication publique. La reprise doit rester utile lorsque l'opérateur ou le point d'entrée est non résolu.

Le tableau conserve l'unité de mesure : des inscriptions dans l'instantané, sans compter des incidents indépendamment vérifiés.

Nom de groupe	Inscriptions	Part	Limite
AKIRA	13	10.7%	Nom d'inscription ; résultats individuels à corroborer
The Gentlemen	9	7.4%	Inscrit sous Thegentlemen dans l'instantané ; aucun opérateur commun déduit avec d'autres marques
Qilin	9	7.4%	Nom d'inscription ; le total n'établit pas l'accès initial
Bravox	8	6.6%	Nom d'inscription ; les affirmations restent des affirmations
Safepay	7	5.7%	Nom d'inscription ; paiement et périmètre des données non résolus
Autres noms	76	62.3%	Autres noms combinés ; aucune alliance implicite
Total	122	100.0%	Distinct de la population officielle de rançongiciels

L'arrondi des parts affichées produit une légère différence avec le total. Celui-ci reprend les nombres sous-jacents d'inscriptions.

Les inscriptions suisses d'extorsion couvrent toute la période étudiée



Source : inscriptions Ransompedia retenues avec étiquette de pays, collectées le 22 novembre 2026. Les dates d'inscription ne sont pas des dates d'incident [S2].

AKIRA

Marque d'inscription de rançongiciel | Revendications d'extorsion ; identité de l'opérateur individuel non résolue

ÉLÉMENTS DISPONIBLES

1 janvier–22 novembre

13 inscriptions suisses dans l'instantané retenu [S2]

PÉRIMÈTRE DES INSCRIPTIONS

Noms d'organisations dans l'instantané suisse

VU DANS LES SOURCES PUBLIQUES

[S2] 13 des 122 inscriptions suisses ; une inscription est une affirmation criminelle.

NOTRE ÉVALUATION

Le total justifie la planification de continuité. Il ne prouve ni chiffrement, ni vol, ni paiement, ni point d'entrée pour chaque organisation.

DEGRÉ DE CONFIANCE

Élevée pour le total retenu ; résultats individuels à corroborer.

Qilin

Marque d'inscription de rançongiciel | Revendications d'extorsion ; identité de l'opérateur individuel non résolue

ÉLÉMENTS DISPONIBLES

1 janvier–22 novembre
9 inscriptions suisses dans l'instantané retenu [S2]

PÉRIMÈTRE DES INSCRIPTIONS

Noms d'organisations dans l'instantané suisse

VU DANS LES SOURCES PUBLIQUES

[S2] 9 des 122 inscriptions suisses ; une inscription est une affirmation criminelle.

NOTRE ÉVALUATION

Le total justifie la planification de continuité. Il ne prouve ni chiffrement, ni vol, ni paiement, ni point d'entrée pour chaque organisation.

DEGRÉ DE CONFIANCE
Élevée pour le total retenu ; résultats individuels à corroborer.

The Gentlemen

Thegentlemen (libellé d'inscription)

Marque d'inscription de rançongiciel | Revendications d'extorsion ; identité de l'opérateur individuel non résolue

ÉLÉMENTS DISPONIBLES

1 janvier–22 novembre
9 inscriptions suisses dans l'instantané retenu [S2]

PÉRIMÈTRE DES INSCRIPTIONS

Noms d'organisations dans l'instantané suisse

VU DANS LES SOURCES PUBLIQUES

[S2] 9 des 122 inscriptions suisses ; une inscription est une affirmation criminelle.

NOTRE ÉVALUATION

Le total justifie la planification de continuité. Il ne prouve ni chiffrement, ni vol, ni paiement, ni point d'entrée pour chaque organisation.

DEGRÉ DE CONFIANCE
Élevée pour le total retenu ; résultats individuels à corroborer.

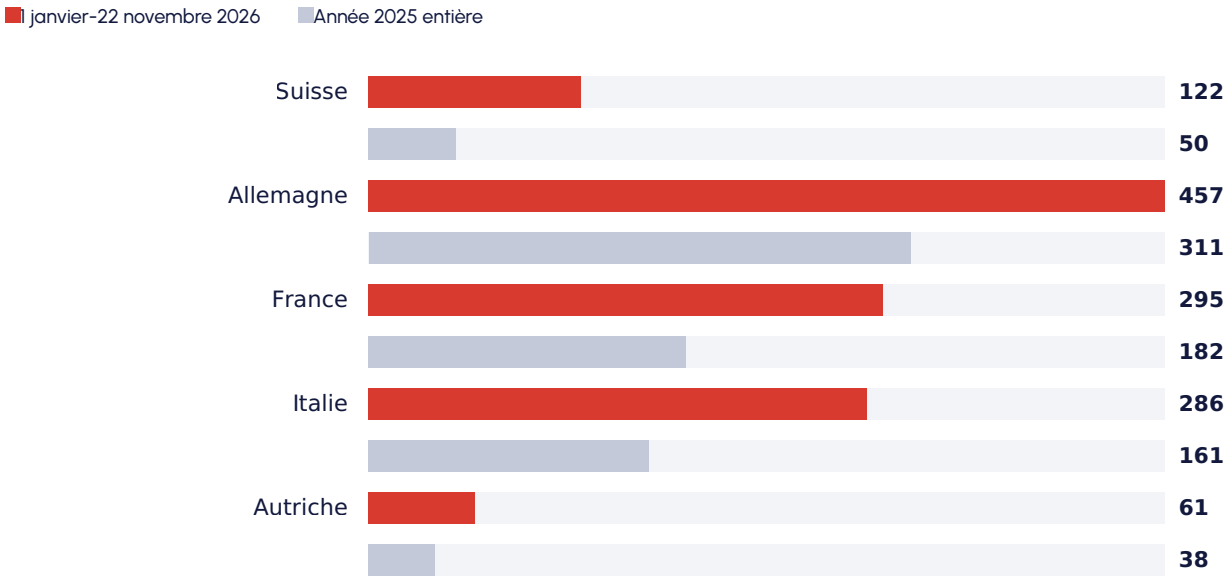
7.2 Contexte régional sans classement des pays

Les voisins sélectionnés partagent frontières, langues ou liens commerciaux avec la Suisse. Leurs totaux sont Allemagne 457, France 295, Italie 286 et Autriche 61. Le même instantané donne pour l'ensemble de 2025 respectivement 311, 182, 161 et 38. Le total suisse de 2025 est 50 [S2].

Les pays de comparaison ont été choisis à titre d'exemples uniquement pour apporter du contexte ; leur sélection n'implique ni classement ni appréciation politique.

Chaque voisin a davantage d'inscriptions partielles en 2026 que sur toute l'année 2025 dans cet instantané. Cette comparaison est descriptive. Périodes, couverture, divulgation et attribution nationale différentes empêchent toute conclusion directe sur les taux d'attaque. Elle n'établit pas qu'un résident ou une entreprise est plus en sécurité dans un pays.

Chaque voisin sélectionné dépasse son total de l'année antérieure complète



Périodes inégales ; pas de classement national des risques. Source : inscriptions Ransompedia retenues avec étiquette de pays, collectées le 22 novembre 2026. Les dates d'inscription ne sont pas des dates d'incident [S2].

Une multinationale peut l'utiliser pour tester un scénario commun de reprise régionale. Un service ou fournisseur partagé peut créer une dépendance transfrontalière même si l'inscription publique ne nomme qu'une entité locale. Le responsable d'incident doit établir le périmètre réel sans reprendre automatiquement l'étiquette nationale.

7.3 Pseudonymes et relations dans les publications retenues

Un pseudonyme est attaché à une publication. Ce n'est ni une personne vérifiée, ni une entreprise, ni une nationalité, ni un opérateur stable. Les fiches conservent seulement les informations nécessaires pour comprendre l'affirmation. Contacts, identifiants de victimes et renseignements personnels sont masqués [S1].

Un pseudonyme répété peut relier des annonces. Il ne prouve pas indépendamment un auteur humain commun, des fichiers identiques ou une vente. Des titres et totaux similaires peuvent aussi résulter de copies publicitaires.

La vue des relations garde donc annonces, pseudonymes et marques comme des nœuds distincts. Une liaison étayée indique ce qui relie deux nœuds. Le graphe affiché contient uniquement deux liaisons observées de pseudonyme vers publication (NormalLeVrai vers B01 et pfavre vers B04), tandis que les trois marques restent non reliées. Le tableau ci-dessous résume les relations de preuve possibles dans le rapport.



Les nœuds séparés n'ont aucune relation établie. Aucun opérateur commun ni alliance n'est déduit.

Relation de preuve possible	Appui	Ce qu'elle n'établit pas
Pseudonyme vers publication	Nom attaché au document retenu [S1]	Identité légale, nationalité ou contrôle de tous les comptes homonymes
Publication vers données annoncées	Description de l'offre [S1]	Authenticité, origine, âge ou personnes uniques
Marque vers inscription	Enregistrement retenu [S2]	Chiffrement, vol, identité d'affilié ou paiement accompli
Autorité vers attribution	Évaluation publiée par l'autorité [S9] [S42]	Attribution indépendante d'une annonce suisse sans lien

NormalLeVrai

Pseudonyme de forum | Rôle publicitaire observé ; identité légale non résolue

ÉLÉMENTS ET CORROBORATION PUBLIQUE

2026-05-04
Annonce présentée dans B01 [S1]

SUJET REVENDIQUÉ

Informations étiquetées assurance

VU DANS LES SOURCES PUBLIQUES

[S1] La publication conservée établit l'annonce. La confirmation indépendante de l'affirmation sous-jacente n'est pas établie ici.

NOTRE ÉVALUATION

Un pseudonyme associé à une offre ne prouve ni personne vérifiée, ni nationalité, ni accès actuel, ni transaction achevée.

DEGRÉ DE CONFIANCE
Élevée pour l'observation du document ; les informations annoncées restent non vérifiées.

pfavre

Pseudonyme de forum | Rôle publicitaire observé ; identité légale non résolue

ÉLÉMENTS ET CORROBORATION PUBLIQUE

2026-11-05
Annonce présentée dans B04 [S1]

SUJET REVENDIQUÉ

Informations de services aux entreprises

VU DANS LES SOURCES PUBLIQUES

[S1] La publication conservée établit l'annonce. La confirmation indépendante de l'affirmation sous-jacente n'est pas établie ici.

NOTRE ÉVALUATION

Un pseudonyme associé à une offre ne prouve ni personne vérifiée, ni nationalité, ni accès actuel, ni transaction achevée.

DEGRÉ DE CONFIANCE
Élevée pour l'observation du document ; les informations annoncées restent non vérifiées.

La progression des informations d'identité vers l'usurpation, les abus de comptes et l'extorsion peut servir de **modèle analytique**. C'est une séquence de planification, sans conclusion de coopération entre pseudonymes et marques du rapport.

7.4 Activité liée à des États selon le SRC

Le rapport 2026 du SRC et la synthèse fédérale désignent les services russes et chinois comme la principale menace d'espionnage en Suisse, aux côtés des cybermenaces étatiques russes, chinoises, iraniennes et nord-coréennes [S9][S110]. L'évaluation officielle distingue le ciblage politique, diplomatique et des infrastructures critiques de la collecte visant les instituts de recherche, universités et entreprises technologiques [S9][S110]. Ces attributions restent celles des autorités suisses ; ce rapport n'attribue ni vendeur anonyme ni inscription non vérifiée à un État.

Le SRC décrit phishing, exploitation de vulnérabilités connues d'équipements réseau et accès par des fournisseurs informatiques ou télécoms. Ce sont des tendances stratégiques d'une évaluation officielle. Elles ne déterminent pas les points d'entrée des incidents sanitaires, fournisseurs ou administratifs du chapitre 5.

Utilisez cette évaluation pour identifier informations sensibles et chemins d'accès persistants. Un institut peut examiner les comptes collaboratifs externes. Une entreprise internationale peut examiner l'accès distant aux informations commerciales sensibles. Un fournisseur peut établir les environnements clients accessibles à ses identités d'assistance.

Axe attribué à la source	Évaluation officielle [S9][S110]	Priorité de décision pour les RSSI
Priorité principale contre l'espionnage	Le SRC identifie les services de renseignement russes et chinois comme principale menace d'espionnage en Suisse	Examiner les accès persistants, espaces diplomatiques ou politiques, et comptes collaboratifs externes
Technologies avancées et recherche	Le SRC souligne la collecte visant universités, instituts de recherche et entreprises technologiques	Auditer les permissions des dépôts de projets, le départ des chercheurs invités et les partages partenaires
Infrastructures critiques et fournisseurs	Le SRC identifie des cyberactivités étatiques contre infrastructures critiques, prestataires informatiques et télécoms	Valider les équipements réseau exposés, la correction des vulnérabilités connues et les accès d'assistance fournisseurs

7.5 Matrice de techniques pour planifier les contrôles

La matrice associe les comportements décrits aux termes ATT&CK. Cette correspondance est une interprétation analytique de planification. Elle n'affirme ni chaîne complète d'attaque ni exécution confirmée dans chaque cas suisse [S9].

Comportement décrit	Terme ATT&CK	Question de planification	Limite
Phishing ciblé	T1566, Phishing [S70]	Les utilisateurs peuvent-ils vérifier l'expéditeur par un canal fiable ?	Tendance décrite par le SRC ; diffusion individuelle distincte
Exploitation d'équipements exposés	T1190, Exploit Public-Facing Application [S71]	Le service a-t-il un responsable, une maintenance et des corrections ?	Un produit vulnérable ne prouve pas son exploitation
Usage d'un compte obtenu	T1078, Valid Accounts [S72]	Sessions, privilèges et récupération sont-ils examinés ?	Possession et usage nécessitent leurs propres preuves

CORRESPONDANCE ANALYTIQUE POUR PLANIFIER LES CONTRÔLES

T1566
Phishing

Tendance décrite par le SRC ; interprétation de planification [S9] [S70]

T1190
Exploit Public-Facing Application

Tendance décrite par le SRC ; interprétation de planification [S9] [S71]

T1078
Valid Accounts

Interprétation de planification exigeant des preuves propres au cas [S72]

Ces termes organisent les demandes de preuves. Ils ne doivent pas devenir une liste décorative de techniques jamais observées. L'équipe incident ne doit établir une technique qu'avec ses propres preuves ou celles de la source citée.

7.6 Préparation aux correctifs : avertissement PHP d'octobre

L'OFCS a émis le 21 octobre 2026 un avertissement urgent pour CVE-2026-109618 et CVE-2026-109619. Il prouve une campagne officielle de correction. Il n'établit aucune exploitation dans une organisation suisse [S62].

Les fiches NVD décrivent corruption mémoire et faiblesses d'état des requêtes. Elles reprennent le score CVSS 4.0 de 9.2 du PHP Group, sans évaluation NVD indépendante. Les avis éditeur identifient les versions touchées et corrigées [S63][S64][S65][S66].

Branche PHP	Versions touchées de la branche	Version corrigée
8.2	Avant 8.2.35	8.2.35
8.3	Avant 8.3.36	8.3.36
8.4	Avant 8.4.27	8.4.27
8.5	Avant 8.5.12	8.5.12

Le tableau présente quatre branches de l'annonce citée. Il n'établit pas l'absence d'effet sur les versions antérieures.

L'éditeur a publié ces versions de sécurité le 21 octobre. Inventoriez les installations intégrées et hébergées, puis vérifiez le composant actif après redémarrage ou redéploiement. Un rétroportage documenté par le fournisseur peut nécessiter une validation distincte du paquet [S67].

Obtenez les mises à jour par le canal établi de l'éditeur, indépendamment d'un message non sollicité.

Une version détectée doit conduire à une décision de correction, sans conclure au vol de données. En cas d'exploitation suspectée, conservez les preuves et examinez le service. Le filtrage peut aider, sans remplacer la validation du logiciel corrigé.

7.7 Acteurs au discours politique

Les DDoS historiques aident les exercices de disponibilité, tout en restant hors du total d'incidents 2026. Le bilan NCSC du sommet de juin 2024 attribuait les DDoS à NoName057(16). Il décrivait des perturbations limitées et séparait les problèmes techniques sans lien des cyberincidents [S42].

La description politique d'un groupe ne prouve pas sa direction par un État. Une annonce coïncidant avec sanctions, réunion internationale ou décision politique n'établit pas indépendamment la cause d'un incident. La réponse doit reposer sur les preuves de service et les responsabilités établies.

7.8 Ce qui renforcerait une évaluation d'acteur

Pour une annonce, des preuves plus fortes relieraient un échantillon authentique à un système et une période pertinents. Pour un accès, elles établiraient compte, privilèges et activité non autorisée. Pour une inscription, elles incluraient le récit propre de l'organisation sur les conséquences de service et de données.

Pour une attribution, elles relieraient infrastructures, comptes, outils ou opérations à un opérateur nommé par une source responsable. Langue et géographie communes sont insuffisantes. Chaque fait doit renforcer une proposition précise, sans transformer tout un pseudonyme en évaluation globale de confiance.

7.9 Altérations temporaires des mises à jour et éléments de preuve rétrospectifs

P

CAS P

Campagne visant les mises à jour d'un logiciel de sauvegarde, avec des répercussions signalées en Suisse (R01)

Chaîne d'approvisionnement logicielle

Incident confirmé par le fournisseur ; victimes suisses non nommées

RÉCIT	Google Threat Intelligence Group et Mandiant décrivent une campagne touchant l'infrastructure de mise à jour d'AOMEI Technology entre avril et juillet 2026. Leur récit inclut la Suisse parmi les pays comptant des organisations touchées. AOMEI reconnaît l'incident concernant son serveur de mise à jour dans sa propre déclaration. [S103][S105]
CHRONOLOGIE	La déclaration du fournisseur a été publiée le 19 octobre et mise à jour le 30 octobre 2026. Elle décrit le renforcement du serveur au plus tard le 29 juillet, une migration le 5 août et la publication de Backupper 8.5.1 le 19 octobre. Ces déclarations datées décrivent la réponse du fournisseur. [S105]
ÉLÉMENTS ÉTABLIS	Les chercheurs décrivent des modifications de configuration durant cinq à dix minutes, avant le rétablissement des contenus légitimes. Ils suivent cette activité sous le nom UNC7017 et décrivent les logiciels malveillants CROSSROAD et SHINYROAD. Ce récit justifie une enquête sur les mises à jour du fournisseur, sans établir de lien avec les profils d'annonceurs ou les marques de rançongiciels de ce rapport. [S103]
LIMITES	Les organisations suisses ne sont pas nommées. La liste des secteurs concernés par l'ensemble de la campagne ne permet pas d'identifier les secteurs touchés en Suisse. Ce rapport ne dispose d'aucun accès aux systèmes des victimes ni d'éléments reliant la campagne à son échantillon d'organisations. Ni les recherches ni la déclaration du fournisseur n'établissent l'existence d'un commanditaire étatique. [S103][S105]

AUTRES EXPLICATIONS	Les chercheurs décrivent une diffusion opportuniste pendant de courtes périodes d'altération. La liste des pays ne permet pas d'établir un ciblage spécifique de la Suisse. Une réponse légitime du serveur de mise à jour observée ultérieurement ne permet pas de déterminer ce qu'un terminal avait reçu auparavant. AOMEI indique poursuivre son évaluation des utilisateurs potentiellement touchés. [S103][S105]
RÉPONSE	Les responsables des logiciels et des terminaux doivent déterminer si le produit était utilisé, conserver l'historique des mises à jour et les journaux des terminaux, puis examiner la période décrite par les sources. Suivez les consignes actuelles du fournisseur concernant l'incident. La seule mise à jour du produit ne remplace pas l'enquête sur une éventuelle exposition antérieure. [S105]

En définitive

Évaluez les livraisons antérieures et l'activité des terminaux séparément de la réponse actuelle du service de mise à jour.

La mesure à retenir est de conserver les éléments de preuve dans les systèmes du fournisseur et de ses clients. La déclaration d'AOMEI distingue explicitement la mise à jour de Backupper de la vérification visant à déterminer si un appareil a été touché. La clôture doit donc examiner séparément les mises à jour reçues auparavant, l'activité des terminaux et l'exposition des comptes concernés. Ces sources ne permettent de déduire aucun nombre de victimes suisses. [S105]

POINTS À RETENIR

01

Traitez marques de rançongiciels, pseudonymes et attributions officielles comme des populations distinctes.

02

Utilisez les techniques pour demander des preuves et tester les contrôles, sans inventer une chaîne d'attaque.

03

Gardez séparés les acteurs sans relation étayée et attribuez les évaluations politiques à leurs sources.

CHAPITRE 08

Économie de la fraude : identité, confiance et paiement

CE CHAPITRE RÉPOND À LA QUESTION

Comment des informations exposées peuvent-elles rendre une demande frauduleuse plus convaincante ?

3

décisions distinctes : identité, autorité et paiement

8.1 Les informations personnelles donnent du contexte, pas d'autorité 73
8.2 Réservations et livraisons transforment le contexte en urgence 73
8.3 Fausse autorité bancaire et paiement physique 74
8.4 Ce qu'établissent les offres clandestines 74
8.5 Données de cartes dans un périmètre étroit 75
8.6 Interrompre la progression à plusieurs étapes 75

CHAPITRE 08

Économie de la fraude : identité, confiance et paiement

EN BREF

Les avertissements officiels montrent comment de vrais détails personnels ou de réservation renforcent une fausse demande. L'attaquant doit encore obtenir confiance, modification d'accès ou paiement. Les offres clandestines décrivent des apports possibles à ce processus, sans fraude accomplie. Gardez les observations de cartes dans leur périmètre étroit, séparées des pertes. Exigez une vérification indépendante lorsqu'une demande inattendue contient des informations exactes.

8.1 Les informations personnelles donnent du contexte, pas d'autorité

L'avis OFCS du 17 novembre décrit du phishing ciblé après une fuite chez un prestataire. Les messages réutilisaient de vrais détails personnels, dont des identifiants d'assurance sociale. Leur exactitude renforçait la crédibilité sans établir l'autorisation de l'expéditeur [S14].

La question de l'assistance change donc. Faire répéter une adresse ou un détail exposé peut confirmer que l'appelant possède l'information. Cela n'établit pas son identité. Un processus plus solide vérifie la demande par un canal fiable existant. Il traite la modification de ce canal comme une action sensible distincte.

Il faut préserver trois propositions. Les données peuvent être authentiques. L'expéditeur peut néanmoins être frauduleux. L'action demandée peut créer une nouvelle perte alors que l'incident initial est contenu. Les fusionner peut conduire à sous-estimer le risque ultérieur.

Le cas du fournisseur de prévoyance apporte un exemple spécifique. Un avertissement policier officiel traite de démarches d'investissement après une fuite chez un tel prestataire. Les informations salariales et de retraite évoquées justifient la préparation aux approches personnalisées. Elles n'établissent pas les champs exacts volés à chaque client du fournisseur [S45].

Il faut préparer les services aux assurés à ces informations convaincantes. Donnez-leur un moyen sûr de vérifier un cas réel et une voie claire de conservation des démarches frauduleuses. Évitez de faire répéter des informations sensibles dans une conversation initiée par un canal inattendu.

8.2 Réservations et livraisons transforment le contexte en urgence

L'avertissement policier de novembre décrit des messages connaissant hébergement et références de réservation. Ils demandaient confirmation puis informations de carte. Connaître une vraie réservation ne prouvait pas que la demande venait du prestataire réservé [S43].

La même distinction vaut pour un message de livraison reçu pendant l'attente d'un colis. Une chronologie familière peut offrir un prétexte convaincant. La mise à jour OFCS du 10 novembre traite des boutiques frauduleuses et du phishing de colis. Elle justifie de vérifier vendeur et message, sans présumer malveillant chaque retard [S13].

Voyagistes, hébergeurs et commerçants doivent permettre la vérification d'une demande inattendue sans son lien ni son numéro. Cette réponse devrait être visible avant un incident. Un portail cohérent, un dossier de réservation et un canal d'assistance aident les clients à résoudre l'incertitude.

Le prestataire doit aussi protéger les comptes d'envoi authentiques. Une demande convaincante peut venir d'un faux domaine, d'un compte détourné ou d'un autre canal. Le message seul n'établit pas la cause en amont. Préservez cette distinction pendant l'enquête.

8.3 Fausse autorité bancaire et paiement physique

L'avertissement policier du 18 novembre décrit des appelants usurpant le personnel bancaire avec une fausse lettre de banque centrale. Ils demandaient des espèces pour un prétendu compte de protection. L'implication revendiquée de la banque centrale appartenait à la tromperie, sans relation établie [S44].

La réponse antifraude doit donc dépasser la connexion en ligne. Un client peut être convaincu de retirer des espèces, déplacer des actifs ou installer un logiciel. Les contrôles du site ne remplacent ni vérification fiable ni escalade des demandes inhabituelles.

La source limite aussi la conclusion. Un avertissement établit la méthode décrite et la préoccupation de l'autorité. Il ne fournit ni pertes nationales estimées ni suivi des consignes par chaque destinataire. Le rapport ne déduit ni l'un ni l'autre de sa publication.

Les banques et autres organisations doivent fournir des formulations capables d'interrompre ce récit. Demandez au client de terminer une conversation inattendue puis de contacter l'organisation par sa voie établie. Le personnel doit éviter de confirmer l'autorité du fraudeur à partir des détails du message suspect.

8.4 Ce qu'établissent les offres clandestines

Les publications retenues comprennent des annonces de comptes, identités, accès et données. Elles peuvent indiquer un intérêt criminel pour un produit. Elles ne prouvent ni transaction conclue, ni émetteur suisse vérifié, ni usage futur par l'acheteur [S1].

La demande B11 proposait $8 pour un compte décrit comme valide par l'annonceur. C'est un paiement proposé, sans transaction observée ni moyenne de marché [S1].

Exemple	Montant annoncé	Unité	Limite
Demande d'achat de compte, B11	$8	Compte décrit comme valide	Paiement et contrôle non vérifiés
Offre d'assurance, B01	Non indiqué dans l'extrait sélectionné	Fichiers et lignes contractuelles	Aucun prix comparable de transaction établi
Offre de prestataire, B04	Non indiqué dans l'extrait sélectionné	Ensemble de données annoncé	L'exclusivité ne prouve pas une vente conclue

Un prix demandé est une condition publicitaire. Il peut varier selon âge, périmètre, exclusivité annoncée, vérification et réputation. Sans preuve de transactions achevées et de produits comparables, un montant ne doit devenir ni perte estimée ni moyenne de marché.

Même règle pour les descriptions d'identité et de compte. Un vendeur peut annoncer compte vérifié, documents ou récupération. Les mots établissent l'offre. Ils ne prouvent ni existence du compte, ni vérification licite, ni contrôle obtenu par l'acheteur.

La première décision défensive est de déterminer si l'affirmation concerne un compte, client ou service propre. La suivante recherche une activité corroborante. L'organisation peut ensuite juger la proportionnalité d'une intervention sur le compte, de contrôles antifraude, d'une assistance client ou d'une réponse élargie.

8.5 Données de cartes dans un périmètre étroit

PORTÉE DES CHIFFRES DES FICHES

Ces observations couvrent uniquement les cartes de paiement apparues en clair dans les publications du dark web retenues pour ce rapport. Brandefense détecte des cartes volées par d'autres moyens, extérieurs à cette section. Ces observations ne mesurent ni vols, ni cartes actives, ni pertes frauduleuses, ni couverture totale de Brandefense.

La population retenue contient 164 cartes distinctes associées à la Suisse, visibles en clair dans 165 publications. Il s'agit uniquement de la population étroite définie ci-dessus [S4].

Une publication peut annoncer une carte fonctionnelle ou montrer une réponse apparente d'outil de vérification. Ce texte reste la représentation de l'auteur. Ce n'est pas un test autorisé par l'émetteur et cela ne prouve aucun débit. Le rapport ne publie ni détails personnels, ni numéros, ni données de cartes exploitables.

L'émetteur recevant un signal pertinent doit le valider par son processus interne. Contact client, restriction ou remplacement dépendent de ses preuves. Une petite population de publications ne permet pas de déterminer si les cartes constituent une source majeure ou mineure des pertes nationales.

8.6 Interrompre la progression à plusieurs étapes

La progression est un **modèle analytique** de planification des contrôles. Elle n'établit aucun opérateur commun derrière les avertissements cités ou annonces retenues.

Étape	Abus possible	Décision	Responsable
Information	Détails personnels ou de réservation réels dans un message	Vérifier séparément l'autorité de l'expéditeur	Service client
Persuasion	Urgence ou rôle institutionnel de confiance revendiqué	Terminer le contact inattendu et utiliser la voie établie	Destinataire et assistance
Identité	Demande de réinitialisation ou de changement de récupération	Vérifier indépendamment le changement sensible	Opérations identité
Paiement	Nouveau bénéficiaire, retrait ou action sur carte	Appliquer l'examen transactionnel et antifraude de l'institution	Opérations antifraude
Suivi	Signalement d'une tentative ou fraude accomplie	Conserver les preuves et évaluer l'exposition restante	Équipes incident et clientèle

Le modèle offre plusieurs occasions d'agir. Une personne ayant divulgué des informations peut encore arrêter un paiement. Un prestataire ayant restauré ses systèmes peut devoir préparer ses clients aux messages ciblés. La clôture technique initiale ne doit donc pas terminer l'assistance antifraude.

POINTS À RETENIR

01

Vérifiez l'autorité séparément de l'exactitude des détails personnels ou de réservation.

02

Traitez prix annoncés et résultats d'outils comme des affirmations, sans déduire ventes ou pertes.

03

Offrez clients et assistance une voie fiable indépendante du message suspect.

CHAPITRE 09

Analyse approfondie de la banque

09

CE CHAPITRE RÉPOND À LA QUESTION

Quelles décisions bancaires relient identité, fraude, fournisseurs et surveillance ?

40

organisations candidates de banque et finance dans la population sélectionnée

9.1 Populations bancaires et d'émetteurs mesurées 78

9.2 Le secret bancaire ne permet pas d'inférer le risque cyber 79

9.3 Relier identité et fraude sans confondre les cas 79

9.4 La détection fournisseur peut lancer l'évaluation prudentielle 79

9.5 Exercice bancaire fondé sur les avertissements cités 80

CHAPITRE 09

Analyse approfondie de la banque

EN BREF

Les 40 organisations bancaires et financières sélectionnées recensent au moins 16 082 associations d'appareils et 1 055 051 associations historiques d'identifiants. Des identifiants associés à 7 étaient proposés à la vente lors de la vérification. Ces observations ne comptent ni clients touchés ni intrusions bancaires confirmées. Sous-ensemble des émetteurs et population étroite de cartes répondent à des questions distinctes. Confiez aux équipes identité, terminaux et antifraude la validation de chaque signal pertinent dans les registres autorisés.

9.1 Populations bancaires et d'émetteurs mesurées

La population comprend 40 organisations candidates de banque et finance. Ce groupe raisonné n'est ni une liste complète de banques agréées ni un échantillon représentatif. Les domaines principaux ne définissent pas chaque filiale, portail client ou fonction externalisée [S3].

Observation	Nombre
Organisations bancaires et financières évaluées	40
Organisations avec annonces actuelles	7
Associations d'appareils, au moins	16 082
Associations d'appareils classés employés	236
Associations historiques d'identifiants	1 055 051

Le sous-ensemble rapproché des émetteurs contient 6 organisations de ce groupe bancaire. Il en compte 4 avec des annonces actuelles d'identifiants, 5 avec des associations d'appareils classés employés et 6 avec des associations hors de cette classification [S3][S4].

Dans ce sous-ensemble, l'instantané contient 208 associations d'appareils classés employés et 12 924 autres associations. Les publications conservées attribuent 7 observations distinctes de cartes en clair à ces émetteurs. Ces populations se chevauchent et diffèrent par leur sens ; elles ne comptent ni clients touchés ni pertes frauduleuses.

Une observation de carte n'établit pas une intrusion chez l'émetteur. Une association d'appareil ne prouve ni propriété, ni infection actuelle, ni compte bancaire encore actif. Validez chaque signal par les processus autorisés d'identité, de terminaux et d'antifraude de l'émetteur.

Les avis officiels de fraude restent des exemples propres aux sources [S14][S44][S45]. Utilisez-les pour tester vérification fiable et escalade transactionnelle. Distinguez les contrôles passifs de configuration de l'indicateur national Atlas et des enquêtes sur les comptes.

9.2 Le secret bancaire ne permet pas d'inférer le risque cyber

Le rapport ne prend position ni sur le secret bancaire ni sur les politiques gouvernementales. Il ne déduit ni posture sécuritaire, ni intérêt d'attaquant, ni cause d'incident d'une description juridique ou politique du secteur. Les éléments concernent des affirmations précises, avertissements officiels et observations de contrôles sélectionnées.

La question opérationnelle bancaire porte sur les informations autorisant accès ou transaction. Connaître adresse, historique de prévoyance ou autre détail privé ne doit pas automatiquement conférer cette autorité. Les avertissements montrent pourquoi contexte exact et instruction frauduleuse peuvent coexister [S14][S44][S45].

Le personnel a besoin d'une voie utilisable de vérification indépendante des informations de l'appelant. Le processus doit couvrir le client urgent, le prétendu cadre demandant une exception et le fournisseur supposé signalant un incident. Chacun exige une confirmation et un responsable différents.

9.3 Relier identité et fraude sans confondre les cas

Une alerte d'identité peut établir une connexion suspecte sans transfert frauduleux. Une alerte de paiement peut établir une transaction inhabituelle sans usage du compte en ligne. Une fuite peut rendre un appel convaincant sans donner accès aux systèmes bancaires.

Le dossier partagé doit conserver ces distinctions. L'identité consigne sessions, récupération et accès applicatifs. L'antifraude consigne bénéficiaire demandé, approbations et état transactionnel. Le service client conserve la communication et décrit la démarche reçue.

Cette vue aide à proportionner la réponse. Révoquer les sessions traite un accès. Examiner un nouveau bénéficiaire en traite un autre. Aider le client à vérifier un message en traite un troisième. Aucune action seule n'établit la résolution complète.

9.4 La détection fournisseur peut lancer l'évaluation prudentielle

Les orientations FINMA intègrent les fonctions externalisées à la responsabilité d'incident de l'établissement. Pour l'obligation décrite, le délai peut commencer lorsque l'établissement ou son fournisseur identifie l'attaque. Il ne faut pas supposer qu'une réunion interne ultérieure déclenche le délai [S8].

Le Moniteur des risques 2025 de la FINMA indique que les annonces concernant des attaques contre des tiers représentaient environ 47% des cyberincidents annoncés à la FINMA sur la période indiquée [S109]. Ce repère prudentiel explique l'importance des exercices d'externalisation dans le secteur financier, sans impliquer un taux d'incidents fournisseurs pour les 40 organisations bancaires et financières sélectionnées [S3][S109].

Testez le premier message fournisseur par un exercice. Il doit identifier fonction touchée, heure de découverte, effets connus, incertitudes et contact de suivi. Conformité et gestion d'incident doivent pouvoir évaluer l'obligation pendant la poursuite de l'enquête technique.

L'établissement doit distinguer annonce prudentielle et autres obligations. Risques personnels et infrastructures critiques ont leurs propres déclencheurs. Un formulaire transmis par un canal ne remplit pas automatiquement toutes les annonces. Le chapitre 10 précise ces différences [S6][S7][S8].

9.5 Exercice bancaire fondé sur les avertissements cités

Utilisez un scénario où un client reçoit un appel citant un vrai incident fournisseur et des détails personnels exacts. L'appelant demande un transfert protecteur ou mouvement d'espèces urgent. Testez ensemble assistance, fraude et identité [S14][S44][S45].

La preuve de réalisation du service client est un canal vérifié indépendamment. Celle de l'antifraude est une décision consignée sur la transaction. Celle de l'identité évalue accès et récupération. Celle de la communication explique clairement les faits connus de l'établissement.

Un second scénario peut commencer par l'alerte d'un prestataire externalisé. Exigez du responsable de service l'identification de la fonction bancaire et du dispositif de continuité. La conformité consigne les obligations. L'infrastructure démontre une restauration indépendante des accès de production du prestataire touché.

Le résultat doit démontrer des décisions, sans déclarer la banque sûre. Un exercice peut révéler contact manquant, déclencheur flou ou compte de reprise indisponible. Ces constats sont exploitables avec responsables et preuves de clôture.

POINTS À RETENIR

01

Distinguez identité, transaction et exposition des données dans un dossier commun.

02

Testez la première alerte fournisseur au regard des responsabilités d'annonce de l'établissement.

03

Faites de la vérification fiable et de la reprise indépendante des contrôles bancaires démontrables.

CHAPITRE 10

Réglementation et réponse nationale

10

CE CHAPITRE RÉPOND À LA QUESTION

Quelles obligations suisses s'appliquent, quand commencent leurs délais et que faut-il préparer ?

24 h

annonce initiale d'infrastructure critique après découverte, si l'obligation s'applique

10.1 Trois obligations possibles pour un incident 82
10.2 Infrastructures critiques : établir le périmètre avant l'incident 83
10.3 Données personnelles : évaluer les dommages aux personnes 83
10.4 Établissements financiers : intégrer la découverte fournisseur au délai 84
10.5 La loi sur la cybersécurité proposée n'est pas une obligation en vigueur 84
10.6 Préparer un dossier de preuves et plusieurs décisions 85

CHAPITRE 10

Réglementation et réponse nationale

EN BREF

La Suisse a des obligations distinctes pour infrastructures critiques, données personnelles et établissements financiers surveillés. Périmètres, délais et compléments diffèrent. L'obligation des infrastructures critiques est en vigueur. La loi sur la cybersécurité proposée reste un projet, avec consultation demandée pour juin 2027. Préparez un dossier d'incident commun aux obligations applicables. Désignez une personne pour transmettre les annonces initiales à temps malgré les faits incomplets.

10.1 Trois obligations possibles pour un incident

Un incident technique peut nécessiter plusieurs évaluations juridiques. La loi sur la sécurité de l'information concerne les cyberattaques d'infrastructures critiques couvertes. L'article 24 de la loi fédérale sur la protection des données concerne violations et risques personnels. Les orientations FINMA concernent les cyberincidents importants d'établissements surveillés [S6][S7][S8].

Ces obligations ont des déclencheurs différents. Elles doivent partager un dossier sans être interchangeables. Le responsable juridique doit justifier l'applicabilité, l'inapplicabilité ou les faits encore nécessaires. Ce chapitre résume les orientations officielles citées, sans constituer un conseil juridique.

Le tableau distingue la décision ouvrant chaque chantier de son exigence principale d'annonce.

Régime	Décision d'applicabilité	Exigence initiale	Exigence complémentaire
Loi sur la sécurité de l'information et ordonnance sur la cybersécurité	Infrastructure critique couverte et cyberattaque soumise à annonce	Annonce au OFCS dans les 24 heures suivant la découverte [S6]	Compléter sous 14 jours calendaires [S12]
Loi fédérale sur la protection des données, article 24	Établir d'abord le droit applicable et l'autorité de surveillance compétente [S106]. Sous compétence du PFPDT, évaluer une violation susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux	Responsable du traitement annonçant au PFPDT dans les meilleurs délais [S7]	Informer les personnes si leur protection l'exige ou sur demande du PFPDT [S7]
Communication FINMA 05/2020, précisée par 03/2024	Établissement surveillé et critères d'annonce remplis	Annonce initiale sous 24 heures [S8]	Annonce complète sous 72 heures sur la plateforme FINMA, selon ses règles de délai [S8]

Le délai financier demande une attention particulière. La FINMA compte les périodes de 24 et 72 heures en jours ouvrables bancaires officiels. Exception pour les attaques graves : l'annonce initiale doit intervenir sous 24 heures même hors jours ouvrables [S8]. Un délai unique simplifié manquerait cette distinction.

10.2 Infrastructures critiques : établir le périmètre avant l'incident

Le OFCS identifie la loi sur la sécurité de l'information et l'ordonnance sur la cybersécurité comme bases de l'obligation [S6]. Elle couvre certaines autorités et organisations, notamment énergie, eau potable, transports et administrations cantonales ou communales. L'ordonnance prévoit des exceptions [S6]. Le secteur seul ne résout pas le statut de chaque organisation.

Le OFCS peut déterminer si une autorité ou organisation intéressée est assujettie. Elle peut demander une décision en cas d'incertitude [S12]. C'est une tâche préparatoire concrète pour juridique et continuité. Consignez réponse, services examinés et contact de réévaluation.

L'événement soumis à annonce doit aussi être évalué. Les orientations couvrent les attaques menaçant le fonctionnement critique, manipulant ou divulguant des informations, longtemps indétectées, ou impliquant chantage, menaces ou contrainte [S12]. Une attaque informatique n'est pas exclue parce que les systèmes industriels continuent de fonctionner.

À l'inverse, le OFCS précise qu'un DDoS sur une application non critique ne déclenche pas automatiquement l'obligation. La question déterminante est la mise en péril du fonctionnement critique [S12]. Le dossier doit donc préciser la fonction métier touchée au-delà des symptômes techniques.

Une enquête incomplète ne suspend pas le délai initial. Le OFCS exige une première annonce sous 24 heures même sans informations complètes. Les compléments peuvent être transmis sous 14 jours calendaires [S12]. Consignez faits confirmés, incertitudes et responsable de la prochaine mise à jour.

L'obligation a débuté le 1 avril 2025. Les sanctions sont entrées en vigueur le 1 octobre 2025, avec amendes possibles jusqu'à CHF 100 000 [S60]. Chaque retard ne produit pas automatiquement une amende. Le récit officiel décrit contact avec l'opérateur, décision formelle puis éventuelle plainte pénale en l'absence persistante de réponse [S60].

10.3 Données personnelles : évaluer les dommages aux personnes

Établissez d'abord le droit applicable en matière de protection des données et l'autorité de surveillance compétente. Le PFPDT surveille les personnes privées et les organes fédéraux. Les autorités cantonales et communales doivent examiner leurs exigences cantonales applicables et l'autorité de surveillance compétente [S106].

Le PFPDT définit une violation par perte, suppression, destruction, modification, divulgation ou accès accidentel ou illicite à des données personnelles [S7]. Une publication publique n'est pas nécessaire. Disponibilité et intégrité comptent aussi avec la confidentialité.

Le responsable du traitement doit annoncer au PFPDT dans les meilleurs délais tout risque élevé vraisemblable pour la personnalité ou les droits fondamentaux [S7]. Il n'existe pas de délai suisse universel de 72 heures. L'évaluation considère les informations et leurs conséquences pour les personnes.

Les orientations déconseillent d'attendre dans le doute si un risque élevé ne peut être suffisamment exclu. Les mesures prévues n'effacent pas la question d'annonce. Le responsable doit documenter connaissances, base d'évaluation et protections déjà étayées [S7].

Annonce à l'autorité et information des personnes sont distinctes. L'article 24 impose l'information individuelle si la protection l'exige ou si le PFPDT la demande [S7]. Le message client doit expliquer faits et actions sans reproduire les informations exposées.

Cette distinction aide pour une affirmation de données clients anciennes. La date publicitaire n'établit pas l'accès aux données. L'organisation doit établir authenticité et protections nécessaires aux personnes. L'évaluation juridique suit les preuves, sans reprendre la description du vendeur.

10.4 Établissements financiers : intégrer la découverte fournisseur au délai

La FINMA attend une première évaluation de criticité dans le délai initial [S8]. Entre compléter cette évaluation et respecter le délai, l'établissement doit privilégier ce dernier. L'annonce initiale peut être retirée si l'enquête montre des critères non remplis.

Pour les fonctions externalisées, le délai commence lorsque l'établissement ou son fournisseur identifie le cyberincident [S8]. Contrat et escalade doivent donc intégrer l'heure de découverte du fournisseur au dossier interne. Attendre son rapport final peut priver l'établissement des informations nécessaires à sa propre obligation.

Les orientations couvrent aussi les prestataires qui ne sont pas des partenaires d'externalisation importants. L'établissement doit recevoir les informations pertinentes et évaluer sa propre obligation [S8]. Un registre limité aux plus gros contrats peut manquer une dépendance opérationnelle.

Les établissements aussi couverts par la loi sur la sécurité de l'information peuvent transmettre l'annonce initiale à la FINMA via le formulaire OFCS, sous réserve de ponctualité. L'annonce complète de 72 heures reste exigée sur la plateforme FINMA de saisie et de demande [S8]. Conservez chaque preuve d'envoi.

Le processus doit être exercé avec la reprise. Les orientations FINMA demandent des exercices par scénarios et distinguent établissements systémiques et autres [S8]. Son bilan de février 2026 souligne aussi scénarios incomplets, responsabilités floues et processus de réponse insuffisamment testés [S61].

Un exercice bancaire utile combine panne fournisseur, accès incertain aux données clients et découverte le week-end. Il vise les décisions initiales requises sans attendre un bilan forensique complet. Testez aussi l'approbation des communications clients et la poursuite des services critiques.

10.5 La loi sur la cybersécurité proposée n'est pas une obligation en vigueur

Le 25 septembre 2026, le Conseil fédéral demandait au DDPS un projet de consultation de loi autonome sur la cybersécurité pour juin 2027 [S11]. L'annonce couvre produits numériques, données numériques importantes et services cloud ou d'hébergement. Elle propose aussi d'y transférer l'obligation existante d'annonce des infrastructures critiques.

L'annonce décrit une législation en développement. Elle n'établit pas l'entrée en vigueur des obligations proposées à la date d'arrêté. La source précise le maintien des règles sectorielles existantes [S11]. Consignez le projet comme veille juridique attribuée, sans échéance opérationnelle déjà applicable.

Le projet cite le règlement européen sur la cyberrésilience comme modèle de règles produits [S11]. Cela ne transforme pas chaque obligation européenne en obligation suisse. Les groupes internationaux doivent examiner entité, service et juridiction applicable. Le rapport ne prend position ni sur ce choix ni sur les relations avec l'Union européenne.

10.6 Préparer un dossier de preuves et plusieurs décisions

Ces préparatifs transforment les régimes séparés en processus utilisable dans l'incertitude.

Préparation	Responsable	Preuve de réalisation
Résoudre statut d'infrastructure critique et exceptions	Juridique et continuité	Applicabilité écrite et date de réévaluation
Consigner découverte interne et chez les prestataires pertinents	Chef d'incident	Dossier horodaté avec incertitudes expliquées
Évaluer personnes et dommages probables	Protection des données	Risques et décision d'annonce documentés
Préparer les annonces initiales malgré les lacunes	Juridique et sécurité	Modèles testés, déposant et suppléant désignés
Confirmer canaux et preuves de réception	Conformité	Accès exercés et confirmations conservées
Exercer défaillance fournisseur avec les métiers	Continuité	Processus alternatif testé, reprise prouvée et corrections attribuées

Le chef d'incident doit séparer observations et conclusions. Affirmation d'acteur, panne, accès non autorisé confirmé et divulgation confirmée peuvent apparaître à différents moments. Chacun peut changer l'évaluation juridique. Le dossier doit montrer décideur et preuves associées.

POINTS À RETENIR

01

L'obligation des infrastructures critiques est en vigueur : annoncez sous 24 heures si applicable et complétez sous 14 jours calendaires.

02

PFPDT et FINMA ont des déclencheurs et délais distincts ; la découverte fournisseur peut lancer le délai financier.

03

La loi proposée reste un sujet de veille ; préparez les obligations actuelles et suivez le projet de consultation.

CHAPITRE 11

Perspectives

11

CE CHAPITRE RÉPOND À LA QUESTION

Quels éléments doivent modifier la prochaine décision de sécurité et cette analyse ?

5

jugements conditionnels avec limites et signaux explicites

11.1 Principaux jugements 87
11.2 Ce qui modifierait l'analyse 88
11.3 Scénarios conditionnels 88
11.4 Un rythme de révision lié aux décisions 89

CHAPITRE 11

Perspectives

EN BREF

Préparez-vous à l'extorsion de données, aux abus d'identité, aux perturbations fournisseurs et à la collecte ciblée d'informations. Les éléments ne donnent aucune probabilité d'attaque individuelle. Évaluations officielles et affirmations observées ont des usages différents. Les scénarios les transforment en décisions attribuées, avec des preuves susceptibles de changer le plan. Réexaminez chaque jugement à l'arrivée de nouveaux éléments propres à l'organisation.

11.1 Principaux jugements

Les jugements concernent les priorités de préparation. La confiance décrit la proposition indiquée, sans évaluer la fiabilité d'un acteur ou la probabilité d'attaque d'une organisation.

Jugement	Confiance	Base et limite	Signal de décision
L'extorsion justifie une reprise métier testée	Élevée pour le besoin préparatoire	Le rapport recense des inscriptions ; le SRC identifie le risque de rançongiciels pour les infrastructures critiques [S2][S9]. Les inscriptions ne confirment pas les incidents individuels	Accès corroboré, reprise compromise ou incident fournisseur pertinent
Recherche sensible et informations politiques nécessitent des contrôles d'accès persistants	Élevée pour l'évaluation source	Le SRC identifie ces cibles, le phishing et l'exploitation d'équipements réseau [S9]. Aucune probabilité d'attaque n'en découle	Accès inexpliqué, partage externe ou contact suspect concernant des travaux sensibles
La découverte fournisseur doit atteindre rapidement le chef d'incident	Élevée pour la dépendance d'annonce	Le délai FINMA d'externalisation peut commencer à la découverte fournisseur [S8]. L'applicabilité dépend de l'établissement et de l'incident	Incident identifié par un prestataire concernant une fonction externalisée
Les événements publics justifient la continuité	Modérée pour le scénario	Le SRC identifie le risque de saturation événementielle ; le sommet 2024 fournit le contexte historique [S9] [S10]. Aucune nouvelle campagne n'est établie	Revendications pertinentes avec anomalies de service ou alertes fournisseurs
La préparation des annonces peut progresser avant de connaître tous les faits	Élevée pour le besoin préparatoire	Les orientations autorisent annonces initiales puis compléments [S8][S12]. Le déclencheur juridique reste à évaluer	Incident potentiellement soumis à annonce avec faits techniques incomplets

La première question est la pertinence pour votre service. Un avertissement national peut justifier une vérification préparatoire. Il n'établit ni compte actif, ni offre authentique, ni détention de vos données par un fournisseur touché. Ces propositions exigent des preuves organisationnelles.

Les priorités diffèrent selon l'activité. Un institut peut prioriser les accès externes de projets. Un prestataire de paiement peut privilégier comptes clients et escalade tierce. Un service public peut nécessiter un processus manuel testé avant un grand événement. Le même contexte national justifie ces choix différents.

11.2 Ce qui modifierait l'analyse

Le tableau identifie les preuves nécessitant une réponse différente. Il précise aussi celles qui réduisent la préoccupation, pour éviter l'urgence permanente après une affirmation non vérifiée.

Nouvel élément	Changement de réponse	Élément réduisant la préoccupation	Responsable
Compte actuel valide dans des éléments pertinents d'exposition	Examiner compte, sessions et historique ; contenir selon les constats	Compte désactivé, information obsolète ou lien organisationnel non étayé	Identité et réponse aux incidents
Fournisseur confirmant l'accès à un environnement contenant des informations propres	Établir périmètre, délais et continuité	Preuves d'absence d'effet sur environnement, données et chemins administratifs concernés	Responsable fournisseur et juridique
Échantillon correspondant aux données internes contrôlées	Ouvrir enquête documentée et évaluation des risques personnels	Divulgation déjà corrigée ou informations publiques, avec risque résiduel évalué	Propriétaire des données et protection des données
Site public pertinent indisponible pendant une campagne	Confirmer l'impact et escalader au prestataire	Preuves internes et fournisseur d'une panne sans lien	Responsable de service et communication
Activité inhabituelle dans un espace sensible de recherche ou politique	Conserver preuves, examiner persistance et partage	Activité autorisée confirmée par le propriétaire et les traces	Propriétaire de l'information et sécurité

Aucun signal n'exige une attribution publique immédiate. Établissez d'abord impact, accès et données. L'attribution peut rester ouverte pendant le confinement et les annonces obligatoires. La communication doit conserver la même incertitude que l'enquête.

11.3 Scénarios conditionnels

Premier scénario conditionnel : panne fournisseur pendant une revendication d'extorsion. C'est une hypothèse de planification. Si le fournisseur soutient un processus critique, activez la continuité convenue tout en évaluant l'accès aux informations. Attribuez restauration métier et question des données à des responsables distincts.

Les premières preuves sont l'heure de découverte fournisseur et les systèmes confirmés touchés. Pour la finance, évaluez la règle d'externalisation sans attendre l'enquête finale [S8]. Pour les autres services critiques couverts, évaluez fonctionnement et déclencheur [S12]. L'exercice se clôt lorsque le processus alternatif approuvé fonctionne et que les risques restants ont des responsables.

Deuxième scénario conditionnel : un acteur cite un enjeu politique et nomme un service public. L'explication reste celle de l'acteur. En cas d'anomalies, vérifiez avec prestataire et métier. Conservez la revendication sans répéter d'injures ni adopter sa position. Communiquez l'impact vérifié propre à l'organisation.

Le bilan historique du sommet montre l'importance des explications séparées : le NCSC distinguait DDoS, tentatives d'intrusion, phishing et problèmes techniques sans lien [S42]. Testez cette séparation. Clôturez lorsque le responsable explique l'interruption, consigne la reprise et précise les inconnues.

Troisième scénario conditionnel : un projet sensible reçoit un contact externe convaincant. Le SRC décrit messages ciblés et contacts par messagerie parmi les techniques d'espionnage [S9]. Si le contact suspect concerne un projet réel, vérifiez l'expéditeur par une voie établie. Examinez les preuves associées d'authentification, partage ou installation.

Le propriétaire décide des restrictions supplémentaires nécessaires aux documents. La sécurité recherche des accès au-delà du premier message. Clôturez lorsque le contact est résolu et chaque compte ou partage concerné a une qualification documentée. Une invitation convaincante seule ne prouve pas une intrusion réussie.

Quatrième scénario conditionnel : des données anciennes sont annoncées comme un nouvel incident. Séparez date publicitaire et date d'accès. Si les données semblent pertinentes, comparez-les aux informations d'incident conservées par des procédures autorisées. Expliquez aux équipes clientes comment de vrais détails anciens facilitent une fraude convaincante.

L'action change si les traces révèlent une nouvelle période d'accès ou un nouveau système. La protection des données réévalue le risque avec les faits nouveaux. Si la divulgation était déjà corrigée, consignez conclusion et précautions antifraude maintenues. La recirculation ne prouve pas un nouvel incident.

11.4 Un rythme de révision lié aux décisions

Attribuez chaque jugement à un responsable de révision dans le processus de risque existant. Mettez-le à jour quand le service ou fournisseur change. Un nouveau total de publications doit susciter un examen, sans escalade automatique du risque métier.

L'indicateur national Atlas décrit le portefeuille évalué. Nombres sectoriels de signaux et observations passives soutiennent différentes tâches de validation. Utilisez les dépendances documentées de services, informations et fournisseurs pour ordonner les travaux. Réévaluez les priorités lorsque validité des comptes, activité pertinente ou impact sur les services sont établis [S3].

La preuve de réalisation est le signe le plus utile de progrès. Service restauré, accès obsolète retiré, canal d'annonce testé ou dépendance résolue modifient la capacité d'action. Une liste croissante d'alertes ne prouve pas l'amélioration de ces résultats.

POINTS À RETENIR

01

Utilisez les perspectives comme planification conditionnelle, sans probabilité d'attaque propre à une organisation.

02

Modifiez la réponse quand les preuves confirment accès pertinent, informations touchées ou impact, en séparant l'attribution.

03

Réexaminez les priorités avec responsables et preuves de réalisation, surtout si la reprise dépend d'un fournisseur.

CHAPITRE 12

Plan d'action

12

CE CHAPITRE RÉPOND À LA QUESTION

Qui agit ensuite et quelles preuves démontrent la réalisation ?

3

périodes de mise en œuvre avec responsables désignés

12.1 Actions du prochain cycle de planification 92
12.2 Identité et réponse aux incidents 93
12.3 Responsables de services et fournisseurs 94
12.4 Équipes fraude et banque 94
12.5 Juridique et communication 95
12.6 Comment Brandefense peut aider 95

CHAPITRE 12

Plan d'action

EN BREF

Transformez le rapport en travaux démontrables. Commencez par validation des comptes, contacts fournisseurs et arbre de décision d'annonce. Exercez ensuite isolement, communication et reprise. Testez enfin la poursuite des activités pendant une interruption essentielle. Chaque action nécessite responsable, condition de déclenchement et preuve de réalisation. Attribuez les responsabilités avant d'acheter une nouvelle source d'alertes.

12.1 Actions du prochain cycle de planification

Ces périodes sont des objectifs préparatoires. Elles ne remplacent pas un délai légal déjà en cours pendant un incident.

30 jours		
Si une nouvelle offre d'identifiants ou d'accès correspond à un compte, valider statut et activité récente	RESPONSABLE Opérations identité	PREUVE DE RÉALISATION Qualification avec statut, sessions, action et faits non résolus
Si un fournisseur essentiel traite des données sensibles, vérifier contact incident et voie d'alerte initiale	RESPONSABLE Achats et responsable de service	PREUVE DE RÉALISATION Contact testé et dépendances données-services consignées
Si un événement peut affecter les opérations essentielles, évaluer les critères d'annonce critique	RESPONSABLE Chef d'incident et juridique	PREUVE DE RÉALISATION Décision de déclenchement, découverte et responsable d'annonce
Si des données personnelles peuvent être touchées, évaluer le risque individuel séparément du service	RESPONSABLE Protection des données	PREUVE DE RÉALISATION Risque et décision d'annonce documentés
Si une institution financière externalise une fonction, confirmer le lancement de l'évaluation prudentielle	RESPONSABLE Conformité et externalisation	PREUVE DE RÉALISATION Alerte fournisseur-institution exercée et horodatée

260 jours

Si l'assistance peut réinitialiser des accès sensibles, tester la vérification par canal distinct

RESPONSABLE
Identité et assistance

PREUVE DE RÉALISATION
Exercice montrant refus sûr ou escalade d'une usurpation

Si un avis client peut être imité, préparer un canal fiable de vérification

RESPONSABLE
Fraude et communication

PREUVE DE RÉALISATION
Canal publié et script téléphonique testé

Si un service public subit des revendications politiques, exercer contrôles et activation des protections

RESPONSABLE
Exploitation et communication

PREUVE DE RÉALISATION
Chronologie distinguant annonce, disponibilité et impact vérifié

Si un incident sous-traitant touche plusieurs unités, exercer un dossier partagé de preuves et décisions

RESPONSABLE
Protection des données et services

PREUVE DE RÉALISATION
Exercice sur table avec conclusion distincte par population

390 jours

Si un service essentiel dépend de l'identité principale, tester une restauration indépendante

RESPONSABLE
Continuité et infrastructure

PREUVE DE RÉALISATION
Restauration approuvée par le métier avec identifiants distincts

Si la reprise dépend d'un fournisseur, tester son rôle avec la restauration interne

RESPONSABLE
Continuité et achats

PREUVE DE RÉALISATION
Exercice commun précisant accès, validation et restitution

Si les affirmations externes reviennent, examiner la cohérence des réouvertures

RESPONSABLE
Renseignement et réponse aux incidents

PREUVE DE RÉALISATION
Échantillon de décisions justifiant clôture ou escalade

12.2 Identité et réponse aux incidents

Commencez par les identités capables d'en modifier d'autres. Assistance, administrateurs délégués et comptes de récupération peuvent changer l'issue d'un phishing. Une connexion solide perd sa valeur si un appelant convaincant remplace son facteur de récupération.

Testez le véritable processus d'assistance. Dans un exercice autorisé, demandez une réinitialisation urgente sous une identité de cadre plausible, avec des détails organisationnels exacts. La preuve est un refus sûr ou une escalade par contact vérifié indépendamment. Un courriel de rappel n'est pas équivalent.

Lorsque l'activité non autorisée est établie, conservez les traces avant qu'une modification d'accès n'efface le contexte. Examinez sessions, permissions applicatives, règles de messagerie et récupération selon le cas. Un changement de mot de passe peut laisser un autre chemin ouvert. Le responsable doit consigner chemins examinés et limites de visibilité.

Le renseignement doit aussi traiter clairement les signaux faibles. Un titre peut désigner un incident historique, annuaire public ou homonyme sans lien. Documentez l'alternative, puis les preuves supplémentaires justifiant une réouverture.

12.3 Responsables de services et fournisseurs

Reliez les résultats métier importants à leurs systèmes, comptes et prestataires. Pour une application publique, incluez soumission et vérification alternatives. Pour la santé, incluez accès clinique et validation des données. Pour la finance, incluez approbation des paiements, clientèle et rapprochement.

Un exercice fournisseur utile commence par un avis incomplet. Le prestataire sait l'accès non autorisé sans savoir si des données sont sorties. Demandez au responsable de service les processus touchés, sans remplacer cette incertitude par une revendication d'attaquant.

Testez ensuite le message suivant. Le prestataire peut-il expliquer les nouvelles preuves, la population cliente concernée et le caractère confirmé ou provisoire des données ? Le client doit pouvoir actualiser son évaluation sans élargir silencieusement la conclusion du prestataire.

Séparez les preuves de reprise et de confidentialité. Un service fonctionnel ne prouve pas la protection maintenue des données. Une allégation non vérifiée ne prouve pas l'arrêt des opérations. Métiers et protection des données nécessitent des faits et décisions distincts.

12.4 Équipes fraude et banque

Utilisez les exemples officiels d'usurpation et de phishing ultérieur pour tester les procédures clientèle. Connaître adresse, numéro d'assurance sociale ou incident fournisseur ne rend pas un appelant fiable. Les détails exacts aident à trouver un dossier, sans autoriser paiement ou changement d'authentification.

Les centres de contact doivent pouvoir transférer la conversation vers un canal fiable approuvé. Le client ne devrait pas suivre le lien d'un message inattendu pour vérifier l'avertissement. Des avis cohérents et une page de vérification accessible indépendamment facilitent la démarche.

L'antifraude doit convenir des suspensions de transaction et de l'implication de la réponse aux incidents. Abus d'identité, fraude de paiement et exposition personnelle peuvent coexister tout en restant des constats distincts. Le dossier conserve les preuves de chaque conclusion.

L'émetteur doit valider les signaux externes de cartes dans son environnement contrôlé. Étiquette ou résultat apparent de vérification ne justifient ni publication de détails de compte ni annonce de pertes. Remplacement et contact client relèvent de ses procédures établies.

12.5 Juridique et communication

Préparez un arbre consignant les déclencheurs de chaque annonce. Incluez première découverte, opérations essentielles touchées, risques personnels probables et exigences prudentielles applicables. Conservez la base des décisions d'applicabilité et de non-applicabilité.

La communication doit avoir les mêmes limites de preuve que l'équipe incident. Une déclaration d'attente utile peut identifier problème de service, enquête et alternatives sans répéter un volume non vérifié. Les suivantes précisent changements et incertitudes restantes.

Appliquez la même discipline aux termes politiques. Décrivez un motif déclaré seulement s'il aide à comprendre la revendication. Attribuez-le au groupe ou à l'autorité citée. Évitez slogans et concomitance politique traitée comme preuve de parrainage.

12.6 Comment Brandefense peut aider

Brandefense réunit Cyber Threat Intelligence, Digital Risk Protection et External Attack Surface Management sur une plateforme [S73]. Pour ce rapport, le lien utile associe signal externe, actifs de l'organisation et validation attribuée.

Le renseignement conserve et évalue les affirmations. La protection des risques numériques aide à comprendre l'abus des marques et communications fiables. La visibilité externe identifie le responsable d'un service et où vérifier une configuration. Rien ne remplace les preuves internes ou l'évaluation d'annonce.

Demandez une démonstration Brandefense fondée sur cette question : comment une nouvelle affirmation atteint-elle le bon responsable et reçoit-elle une qualification documentée ? Confirmez périmètre produit et modalités de service pendant cet échange.

POINTS À RETENIR

01

Donnez à chaque action responsable, déclencheur et preuve démontrable.

02

Exercez ensemble fournisseurs, récupération d'identité et restauration métier.

03

Rattachez délais légaux et déclarations publiques à leurs propres faits et déclencheurs.

ANNEXES

Annexes

A–D

CE CHAPITRE RÉPOND À LA QUESTION

Comment interpréter les éléments et remonter à leur source ?

4

annexes sur périmètre, preuves, sources et termes

Annexe A. Périmètre, sources et confiance 97

Annexe B. Registre des éléments 99

Annexe C. Sources 101

Annexe D. Glossaire 106

Annexe A. Périmètre, sources et confiance

Les pays de comparaison ont été choisis à titre d'exemples uniquement pour apporter du contexte ; leur sélection n'implique ni classement ni appréciation politique.

A.1 Période et sens des horodatages

Le rapport couvre le 1 janvier–22 novembre 2026. Les documents clandestins sont datés par publication, sans utiliser la découverte par le lecteur. L'activité récente couvre le 9–22 novembre. Un incident ancien dans une nouvelle publication reste ancien, sauf preuve d'un nouvel événement.

Les données et lectures reflètent la disponibilité à la collecte. Le jour d'arrêté était encore en cours pendant la préparation. Une publication ultérieure ce même jour peut exiger une mise à jour. Le rapport ne déduit pas d'inactivité d'une observation absente.

Les observations passives ont leur propre instant de collecte. Elles ne prouvent pas une configuration identique pendant toute la période. Les dates d'inscription de rançongiciels ne prouvent pas non plus la date d'intrusion. Les avis officiels peuvent traiter d'un fait antérieur ou réviser une estimation.

Les chiffres de publications incluent les contenus datés jusqu'à 07:20 UTC le 22 novembre 2026. La journée de clôture demandée reste ouverte.

A.2 Populations de sources

Le rapport associe publications clandestines retenues par Odin by Brandefense, inscriptions publiques de rançongiciels, observations passives DNS et TLS, observations de sécurité web et informations publiques. Chaque source apporte un type distinct d'éléments [S1][S2][S3].

Une publication consigne annonce, demande ou discussion. Elle ne prouve ni authenticité des données, ni accès actuel, ni transaction achevée. Des offres répétées peuvent décrire les mêmes données alléguées. Lignes, enregistrements, comptes et personnes sont des unités différentes.

Une inscription consigne une affirmation criminelle associée à une organisation et un groupe. Elle ne confirme pas indépendamment chiffrement, extraction, paiement ou victime unique. Les cas officiels constituent une population distincte avec leurs propres signalements et observations [S2][S5].

L'information officielle établit la communication de l'organisation ou autorité nommée. Elle ne donne pas accès aux preuves forensiques internes. Si la source laisse une question ouverte, la fiche et le point à retenir conservent l'incertitude.

A.3 Sélection des organisations et mesures manquantes

La population comprend 250 organisations candidates dans treize secteurs. Cette sélection raisonnée inclut certaines entités liées et des autorités partageant un domaine parent. Elle n'est ni classement national ni échantillon statistiquement indépendant [S3].

Les contrôles passifs couvrent 246 des 250 organisations sélectionnées (en omettant une organisation dans chacun des secteurs banque et finance, administration publique, formation et recherche, et santé) et distinguent réponses non concluantes et échecs.

Les observations d'exposition couvrent séparément 247 des 250 organisations sélectionnées, sans une organisation chacune dans énergie et services collectifs, transport et logistique, et services aux entreprises et aux consommateurs. Les quatre omissions passives et trois omissions d'exposition ne se recoupent pas, laissant 243 organisations dans les deux populations. L'indicateur national Atlas atteint 48 sur 100 pour le portefeuille évalué. Seul le chiffre national Atlas est publié. Les associations d'appareils et d'identifiants peuvent se chevaucher entre organisations et dates. Elles ne comptent ni personnes distinctes ni incidents confirmés [S3].

A.4 Périmètre des cartes

Les observations couvrent seulement les cartes apparues en clair dans les publications retenues. Brandefense détecte des cartes volées par d'autres moyens, hors de cette section. Ces observations ne mesurent ni vol, ni cartes actives, ni pertes, ni couverture totale de Brandefense [S4].

La population de cartes ne doit pas être ajoutée aux identifiants, appareils ou personnes. Le résultat apparent d'un outil reste une affirmation. Toute intervention exige une validation par l'émetteur selon son processus établi.

A.5 Confiance et autres explications

La confiance porte sur une proposition. Le rapport peut être certain d'une annonce observée sans établir son authenticité. Il peut être certain d'une divulgation d'incident sans connaître population finale et périmètre des données.

Un pseudonyme n'est pas une personne vérifiée. Langue, hébergement, titre similaire ou rhétorique politique ne prouvent pas de contrôle commun. Une relation est formulée au niveau étayé. Une séquence de planification sans lien opérationnel établi est étiquetée modèle analytique.

Les scénarios conditionnels du chapitre 11 sont des hypothèses préparatoires. Ils identifient les preuves renforçant ou affaiblissant le jugement. Ils ne chiffrent pas les probabilités d'attaque et ne promettent pas l'efficacité des contrôles.

A.6 Noms publics et neutralité

Les organisations sont nommées dans les récits d'incident seulement avec confirmation officielle et couverture médiatique élargie. Les autres cibles et tiers utilisent des rôles larges. Si le lien d'un média tiers identifierait une organisation masquée, l'entrée publique indique la racine du site de l'éditeur et masque l'URL de l'article. Lorsque l'éditeur est lui-même l'organisation ou l'autorité masquée, l'entrée identifie son rôle et omet l'URL.

Le rapport ne prend position ni sur décisions gouvernementales, secret bancaire, sanctions, relations européennes ou réunions internationales. Les attributions étatiques et d'acteurs restent celles des sources citées. Slogans et descriptions orientées sont omis.

Annexe B. Registre des éléments

Le registre renvoie aux éléments présentés dans les chapitres. Les identifiants restent identiques dans toutes les éditions. Une fiche établit la conservation du document, sans valider l'affirmation.

Fiche	Date	Lieu	Pseudonyme	Langue	Chapitre
B01	2026-05-04	Forum de partage de données	NormalLeVrai	Anglais	4
B02	2026-03-10	Réponse citant une offre	john2samira, citant Niphra	Anglais	4
B03	2026-03-10	Discussion de forum	jb75	Anglais	4
B04	2026-11-05	Forum de vente de données	pfavre	Anglais	4
B05	2026-10-11	Forum de partage de données	updap	Anglais	4
B06	2026-01-06	Demande d'achat sur forum	xmrlover76	Anglais	4
B07	2026-01-27	Forum de partage d'identifiants	thejackal101	Anglais	4
B08	2026-11-07	Forum de vente de données	RummRif	Anglais	4
B09	2026-01-18	Forum de partage de données	Cod3xx	Anglais	4
B10	2026-01-30	Forum de partage de données	hexvior	Anglais	4
B11	2026-04-17	Forum d'achat de comptes	kleinanzeige	Russe et anglais	4
B12	2026-11-19	Annonce de forum	Jlkrumholz01	Anglais	4

Le registre suivant sépare les fiches officielles des publications clandestines. Communications officielles et annonces criminelles ne doivent pas être fusionnées en un total d'incidents.

Fiche	Date	Sujet	Éléments	Chapitre
O01 / Cas F	2026-11-20	Permis cantonaux	Récit officiel ; limites dans la fiche	5
O02 / Cas G	2026-04-30	Continuité radiologique	Récit officiel ; limites dans la fiche	5

Fiche	Date	Sujet	Éléments	Chapitre
O03 / Cas H	2026-10-23	Logiciels de prévoyance	Récit officiel ; limites dans la fiche	5
O04 / Cas I	2026-09-28	Données historiques de personnel médiatique	Récit officiel ; limites dans la fiche	5
O05 / Cas J	2026-07-15	Données de prestataire énergétique	Récit officiel ; limites dans la fiche	5
O06 / Cas K	2026-11-12	Commandes frigorifiques	Récit officiel ; limites dans la fiche	5
O07 / Cas L	2026-08-04	Comptes collaboratifs fédéraux	Récit officiel ; limites dans la fiche	5
O08 / Cas M	2026-10-26	Assistance informatique scolaire	Récit officiel ; limites dans la fiche	5
O09 / Cas N	2026-04-11	Données de formation d'adultes	Récit officiel ; limites dans la fiche	5
O10 / Cas O	2026-11-19	Formulaires universitaires	Récit officiel ; limites dans la fiche	5
R01 / Cas P	2026-10-19	Campagne via les mises à jour d'un logiciel de sauvegarde	Déclaration du fournisseur et recherche primaire ; victimes suisses non nommées	7

Annexe C. Sources

Les numéros de sources qui n'apparaissent pas ont été retirés lors de la révision et ne sont pas cités. Les pages externes et passages justificatifs ont été lus pendant la préparation. Les dates de vérification décrivent cette lecture sans garantir la stabilité des pages. Les entrées propres identifient la population utilisée dans cette édition.

S1: Odin by Brandefense. Odin by Brandefense retained Switzerland-related post material, post window 1 January–22 November 2026 through 07:20 UTC. Own-source population. Verified on 22 November 2026.

S2: Brandefense. Ransompedia listing snapshot for Switzerland and regional peers, collected 22 November 2026. Own-source population. Verified on 22 November 2026.

S3: Odin by Brandefense. Selected organisation universe, Atlas exposure observations read 21–22 November 2026, and passive DNS, TLS and web-security observations collected 22 November 2026. Own-source population. Verified on 22 November 2026.

S4: Brandefense. Clear-text payment-card aggregates from the retained post population. Own-source population. Verified on 22 November 2026.

S5: Federal Office for Cyber Security. First semi-annual cyber report 2026. https://www.bacs.admin.ch/en/hjb-26-1-en. Verified on 22 November 2026.

S6: Federal Office for Cyber Security. Reporting obligation for cyberattacks on critical infrastructure. https://www.bacs.admin.ch/en/reporting-obligation. Verified on 22 November 2026.

S7: FDPIC. Guidelines on reporting data security breaches and informing affected persons under Article 24 FADP. https://www.edoeb.admin.ch/dam/en/sd-web/T64CAUyvAMcF/1_2%20Leitfaden%20des%20ED%C3%96B%20betreffend%20der%20Meldung%20von%20Datensicherheitsverletzungen%20und%20Information%20der%20Betroffenen%20nach%20Art.%2024%20DSG_EN.pdf. Verified on 22 November 2026.

S8: FINMA. FINMA Guidance 03/2024: Cyber risks. https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20160707-finma-aufsichtsmitteilung-03-2024.pdf?sc_lang=en&hash=A1A633E2246BE27B2020897E1A389049. Verified on 22 November 2026.

S9: Federal Intelligence Service. Switzerland's Security 2026. https://www.vbs.admin.ch/dam/en/sd-web/tfhqKbM8ZL5k/VBS-DDPS-NDB-Sicherheit-Schweiz-2026-en.pdf. Verified on 22 November 2026.

S10: Swiss Confederation. First report on the Cyber Situation Network for the Summit on Peace in Ukraine. https://www.europa.eda.admin.ch/en/nsb?id=101528. Verified on 22 November 2026.

S11: Swiss Confederation. Federal Council plans to introduce new Cybersecurity Act. https://www.emek.admin.ch/en/newnsb/zX9oNK8tuI-Z. Verified on 22 November 2026.

S12: Federal Office for Cyber Security. FAQ on the reporting obligation. https://www.bacs.admin.ch/en/faq-reporting-obligation. Verified on 22 November 2026.

S13: Federal Office for Cyber Security. Woche 45: Black Friday wirft seine Schatten voraus – KI-Fakeshops und Paket-Phishing. https://www.bacs.admin.ch/de/26w45-de. Verified on 22 November 2026.

S14: Federal Office for Cyber Security. Woche 46: Personalisiertes Phishing aufgrund von abgeflossenen Daten. https://www.bacs.admin.ch/de/26w46-de. Verified on 22 November 2026.

S15: FDPIC. EDÖB leitete nach Cyberangriff auf Softwarelieferant Abklärungen ein. https://www.edoeb.admin.ch/de/edoeb-leitete-nach-cyberangriff-auf-softwarelieferant-abklaerungen-ein. Verified on 22 November 2026.

S16: Canton of Basel-Landschaft. FAQ-Data - Kanton Basel-Landschaft. https://www.baselland.ch/politik-und-behorden/direktionen/sicherheitsdirektion/amt_fuer_migration/bewilligungen/faq-data/. Verified on 22 November 2026.

S17: Canton of Basel-Landschaft. Cyberangriff auf die IT-Infrastruktur der kantonalen Verwaltung führte zu Datenabfluss - Kanton Basel-Landschaft. https://www.baselland.ch/politik-und-behorden/besondere-behoerden/landeskanzlei/medienmitteilungen/cyberangriff-auf-die-it-infrastruktur-der-kantonalen-verwaltung-fuehrte-zu-datenabfluss. Verified on 22 November 2026.

S18: Groupe 3R. Informations sur la cyberattaque d'avril 2026 - 3R - Réseau Radiologique Romand. https://www.groupe3r.ch/fr/informations-importantes/infos-cyberattaque-avril-2026-7268/. Verified on 22 November 2026.

S19: ICTjournal. Données volées, systèmes rétablis: le Groupe 3R fait le point après la cyberattaque (update) | ICTjournal. https://www.ictjournal.ch/news/2026-07-06/donnees-volees-systemes-retablis-le-groupe-3r-fait-le-point-apres-la-cyberattaque. Verified on 22 November 2026.

S20: SRG. SRG von Cybervorfall betroffen | SRG SSR. https://www.srgssr.ch/de/news-medien/news/srg-von-cybervorfall-betroffen. Verified on 22 November 2026.

S21: Publica. Cyber attack on Publica software supplier: data leak confirmed | PUBLICA. https://www.publica.ch/en/about-us/news/cyber-attack-publica-software-supplier-data-leak-confirmed. Verified on 22 November 2026.

S22: Netzwoche. Salt bestätigt Netzwerkausfall durch Cyberangriff | Netzwoche. https://www.netzwoche.ch/news/2026-05-18/salt-bestaetigt-netzwerkausfall-durch-cyberangriff. Verified on 22 November 2026.

S24: Federal Office for Cyber Security. Woche 5: Weltweite «SharePoint»-Phishing-Welle – auch die Schweiz ist betroffen. https://www.bacs.admin.ch/de/26w5-de. Verified on 22 November 2026.

S25: Federal Office for Cyber Security. Woche 6: «Subscription Bombing» – Wenn das E-Mail-Postfach unter Beschuss steht. https://www.bacs.admin.ch/de/26w6-de. Verified on 22 November 2026.

S26: Federal Office for Cyber Security. Woche 8: «ClickFix» – Wenn eine vermeintliche Fehlerbehebung oder Verifikation eine Malware installiert. https://www.bacs.admin.ch/de/26w8-de. Verified on 22 November 2026.

S27: Federal Office for Cyber Security. Woche 15: Falsche Bankmitarbeiter fordern Installation von Fernwartungssoftware. https://www.bacs.admin.ch/de/26w15-de. Verified on 22 November 2026.

S28: Federal Office for Cyber Security. Woche 18: Paket-Phishing mit perfider Fortsetzung – Die Masche des «Double Phishing». https://www.bacs.admin.ch/de/26w18-de. Verified on 22 November 2026.

S30: Federal Office for Cyber Security. Woche 23: Stellensuchende im Visier – Phishing, Betrug und Schadsoftware im Bewerbungsprozess. https://www.bacs.admin.ch/de/26w23-de. Verified on 22 November 2026.

S32: Federal Office for Cyber Security. Woche 35: Skimming bei Essenslieferdienst - Statt einem vollen Magen eine leere Kreditkarte. https://www.bacs.admin.ch/de/26w35-de. Verified on 22 November 2026.

S34: Federal Office for Cyber Security. Woche 42: Neue Variante von Phishing in Zusammenhang mit Hotelbuchungen zielt auf TWINT-Konten. https://www.bacs.admin.ch/de/26w42-de. Verified on 22 November 2026.

S40: IWB. Adressdaten bei Dienstleister von IWB entwendet (15 July 2026). https://www.iwb.ch/ueber-uns/newsroom/medienmitteilungen/artikel~_adressdaten-bei-dienstleister-von-iwb-entwendet~. Verified on 22 November 2026.

S41: Swiss police cybercrime portal. cybercrimepolice.ch | Cyberangriffe auf Kühlanlagen zeigen die.... https://cybercrimepolice.ch/de/faelle/cyberangriffe-auf-kuehlanlagen-zeigen-die-risiken-vernetzter-geraete. Verified on 22 November 2026.

S42: Federal Office for Cyber Security. Summit on Peace in Ukraine: first NCSC report on Cyber Situation Network. https://www.bacs.admin.ch/en/24-kfu-2-en. Verified on 22 November 2026.

S43: Official public source. Official incident or campaign account concerning a withheld organisation. https://cybercrimepolice.ch/ (article URL withheld). Verified on 22 November 2026.

S44: Swiss police cybercrime portal. cybercrimepolice.ch | Falsches Bankpersonal fordert Bargeld für.... https://cybercrimepolice.ch/de/faelle/falsches-bankpersonal-fordert-bargeld-fuer-angebliches-snb-sicherungskonto. Verified on 22 November 2026.

S45: Swiss police cybercrime portal. cybercrimepolice.ch | Betrügerische Investitionsanrufe nach.... https://cybercrimepolice.ch/de/faelle/betrugerische-investitionsanrufe-nach-datenabfluss-bei-pensionskassendienstleister. Verified on 22 November 2026.

S47: Canton of Basel-Landschaft. Update zum Cyberangriff auf die IT-Infrastruktur der kantonalen Verwaltung Basel-Landschaft - Kanton Basel-Landschaft. https://www.baselland.ch/politik-und-behorden/besondere-behoerden/landeskanzlei/medienmitteilungen/update-zum-cyberangriff-auf-die-it-infrastruktur-der-kantonalen-verwaltung-basel-landschaft. Verified on 22 November 2026.

S48: Netzwoche. Public reporting on an incident concerning a withheld organisation. https://www.netzwoche.ch/ (article URL withheld). Verified on 22 November 2026.

S49: Netzwoche. Public reporting on an incident concerning a withheld organisation. https://www.netzwoche.ch/ (article URL withheld). Verified on 22 November 2026.

S50: Netzwoche. Public reporting on an incident concerning a withheld organisation. https://www.netzwoche.ch/ (article URL withheld). Verified on 22 November 2026.

S53: Federal Office for Cyber Security. Kühl- und Kältesteuerungen: Systeme identifizieren, aktualisieren und schützen. https://www.bacs.admin.ch/de/warnung-kuehlanlagen-de. Verified on 22 November 2026.

S54: Swiss Confederation. Cyberangriff auf SharePoint-Server. https://www.admin.ch/de/newnsb/1CjmpBBHQaMV82PjKEpcL. Verified on 22 November 2026.

S55: Swiss Confederation. Cyberangriff auf Softwarelieferanten: Publica lässt Umgang mit Personendaten und Sicherheitskontrollen extern untersuchen. https://www.admin.ch/de/newnsb/A40p0VPerHSv. Verified on 22 November 2026.

S56: IT-Markt. Public reporting on an incident concerning a withheld organisation. https://www.it-markt.ch/ (article URL withheld). Verified on 22 November 2026.

S57: Netzwoche. Public reporting on an incident concerning a withheld organisation. https://www.netzwoche.ch/ (article URL withheld). Verified on 22 November 2026.

S58: Ifage. Information relative à un incident de sécurité impliquant des données personnelles | ifage. https://www.ifage.ch/news/2026/information-relative-a-un-incident-de-securite-impliquant-des-donnees-personnelles/. Verified on 22 November 2026.

S59: Canton of Vaud. La plateforme de support informatique des Gymnases et des Ecoles professionnelles du Canton victime d'un vol de données | État de Vaud. https://www.vd.ch/actualites/communiques-de-presse-de-letat-de-vaud/detail/communique/la-plateforme-de-support-informatique-des-gymnases-et-des-ecoles-professionnelles-du-canton-victime-dun-vol-de-donnees. Verified on 22 November 2026.

S60: Swiss government / NCSC. Six-month reporting obligation for cyberattacks on critical infrastructures. https://www.admin.ch/en/newnsb/gezctyF6KYR7UkCjXBC5s. Verified on 22 November 2026.

S61: FINMA. How FINMA is getting to the bottom of cyber risks in the financial sector. https://www.finma.ch/en/finma-public/article-series,-c-,-finma-at-work/artikelserie/cyberrisiken/. Verified on 22 November 2026.

S62: BACS warning. Kritische Schwachstellen in PHP: Sicherheitsupdates sofort einspielen. https://www.bacs.admin.ch/de/warnung-php-de. Verified on 22 November 2026.

S63: NVD record. NVD CVE-2026-109618. https://nvd.nist.gov/vuln/detail/CVE-2026-109618. Verified on 22 November 2026.

S64: NVD record. NVD CVE-2026-109619. https://nvd.nist.gov/vuln/detail/CVE-2026-109619. Verified on 22 November 2026.

S65: PHP vendor advisory. PHP security advisory: RCE via OOM corruption. https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w. Verified on 22 November 2026.

S66: PHP vendor advisory. PHP security advisory: RCE via stale global state. https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp. Verified on 22 November 2026.

S67: PHP release announcement. PHP security releases of 21 October 2026. https://www.php.net/archive/2026.php#2026-10-21-5. Verified on 22 November 2026.

S70: MITRE ATT&CK. Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1566/. Verified on 22 November 2026.

S71: MITRE ATT&CK. Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1190/. Verified on 22 November 2026.

S72: MITRE ATT&CK. Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1078/. Verified on 22 November 2026.

S73: Brandefense. Request a Demo | See AI-Driven Threat Intelligence in Action. https://brandefense.io/request-a-demo/. Verified on 22 November 2026.

S80: Università della Svizzera italiana. Incidente di sicurezza informatica – Informazioni e aggiornamenti | USI. https://www.usi.ch/it/data-breach. Verified on 22 November 2026.

S81: Withheld residential care provider. Public incident notices on the July 2026 ransomware disruption and October 2026 recovery update. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S82: FDPIC. Warnung vor betrügerischen E-Mails im Namen des EDÖB. https://www.edoeb.admin.ch/de/warnung-vor-betruegerischen-e-mails-im-namen-des-edoeb. Verified on 22 November 2026.

S83: Withheld Swiss public authority. Public notice on temporary service restrictions during October 2026 PHP vulnerability remediation. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S84: Canton of Vaud. Revue des cybermenaces : Juillet 2026 | État de Vaud. https://www.vd.ch/actualites/actualite/news/26508-revue-des-cybermenaces-juillet-2026. Verified on 22 November 2026.

S85: Canton of Vaud. Revue des cybermenaces : Septembre 2026 | État de Vaud. https://www.vd.ch/actualites/actualite/news/26702-revue-des-cybermenaces-septembre-2026. Verified on 22 November 2026.

S86: Withheld Swiss municipal administration. Public notice of 14 March 2026 on partial encryption and service restoration. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S87: Withheld Swiss sports federation. Public notice of 31 October 2026 on a personal-data incident affecting a licensing platform. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S88: Withheld Swiss sports federation. Public notice of 26 October 2026 on unauthorised account access affecting an administration platform. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S89: Report URI. Vendor research on an incident concerning a withheld organisation. https://blog.report-uri.com/ (article URL withheld). Verified on 22 November 2026.

S90: Withheld cantonal authority. Public notice of 5 August 2026 on a SharePoint incident and precautionary website update. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S91: Withheld cantonal authorities. Joint public notice of 28 August 2026 on automated collection of public vehicle-holder information across five cantons. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S92: Canton of Vaud. Vaud false-bank and false-police fraud update. https://www.vd.ch/actualites/actualite/news/25944-escroquerie-aux-faux-banquiers-policiers-le-nombre-de-cas-repart-a-la-hausse. Verified on 22 November 2026.

S93: Official or public reporting. St.Gallen remote-access fraud warning. https://www.sg.ch/news/sgch_kantonspolizei/2026/02/kanton-st-gallen--betrugsmasche-richtet-grossen-schaden-an.html. Verified on 22 November 2026.

S94: Official or public reporting. Ticino attempted family-emergency fraud. https://www4.ti.ch/di/pol-new/comunicazioni/comunicati-stampa-1/dettaglio/?user_polizia_pi1%5BnewsId%5D=259127. Verified on 22 November 2026.

S95: Official or public reporting. Bern remote-access fraud warning. https://www.police.be.ch/de/start/themen/news/medienmitteilungen.html?newsID=5cd77d2d-9a47-459f-b91d-60e5b6d54a5b. Verified on 22 November 2026.

S96: Official or public reporting. Schaffhausen suspected courier recruitment. https://www.shpol.ch/CMS/Webseite/Schaffhauser-Polizei-23813465-DE.html. Verified on 22 November 2026.

S97: Official or public reporting. Fribourg false-bank messages and card collection. https://www.fr.ch/dsjs/pol/actualites/escroqueries-aux-faux-banquiers-trois-auteurs-presumes-mis-en-cause. Verified on 22 November 2026.

S98: Official or public reporting. Neuchatel false-police and false-bank prevention. https://www.ne.ch/communiques-de-presse/escroquerie-au-faux-policier-et-faux-banquier-la-police-neuchateloise-la-rencontre-de-la-population-du-2-au-7-novembre-2026. Verified on 22 November 2026.

S99: Official or public reporting. Valais false-police and false-bank fraud. https://www.policevalais.ch/communiques-pour-les-medias/arnaque-aux-faux-policiers-pres-de-deux-tiers-des-escroqueries-dejouees/. Verified on 22 November 2026.

S100: Official or public reporting. Zug two courier investigations. https://zg.ch/de/zuger-polizei-news/2026/November/137-kanton-zug-telefonbetrug-zwei-geldkuriere-festgenommen. Verified on 22 November 2026.

S101: Threema. DDoS Attacks on Threema. https://threema.com/en/blog/outage-august-2026. Verified on 22 November 2026.

S102: SC Media. Encrypted messaging provider Threema hit by large-scale DDoS attacks. https://www.scworld.com/brief/encrypted-messaging-provider-threema-hit-by-large-scale-ddos-attacks. Verified on 22 November 2026.

S103: Google Threat Intelligence Group and Mandiant. Investigating Ephemeral Supply Chain Tampering. https://cloud.google.com/blog/topics/threat-intelligence/investigating-ephemeral-supply-chain-tampering. Verified on 22 November 2026.

S105: AOMEI. Statement on Ephemeral Tampering with the AOMEI Backupper Update Server. https://www.aomeitech.com/company/investigating-ephemeral-tampering.html. Verified on 22 November 2026.

S106: FDPIC. Tasks: data protection. https://www.edoeb.admin.ch/en/tasks-data-protection. Verified on 22 November 2026.

S107: Federal Office for Cyber Security. Semi-Annual Report 2025/2 (30 March 2026). https://www.bacs.admin.ch/en/hjb-25-2-en. Verified on 23 November 2026.

S108: Federal Office for Cyber Security. Semi-Annual Report 2025/1 (18 November 2025). https://www.bacs.admin.ch/en/hjb-25-1-en. Verified on 23 November 2026.

S109: FINMA. FINMA Risk Monitor 2025 (17 November 2025). https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/risikomonitor/20251117-finma-risikomonitor-2025.pdf?hash=6CB0C57B5333208BA29F26542B3B76B8&sc_lang=en. Verified on 23 November 2026.

S110: Swiss Confederation. «Sicherheit Schweiz 2026»: Keine Entwarnung für die Schweiz (25 June 2026). https://www.wbf.admin.ch/de/newnsb/jyRmuld1hBVy. Verified on 23 November 2026.

Annexe D. Glossaire

- **BACS / NCSC :** Office fédéral de la cybersécurité (OFCS) ; BACS est l'abréviation allemande, NCSC celle utilisée dans les documents anglais [S6].
- **FDPIC / EDÖB :** Préposé fédéral à la protection des données et à la transparence (PFPDT) ; les abréviations anglaise et allemande désignent la même autorité [S7].
- **FINMA :** Autorité fédérale de surveillance des marchés financiers, avec exigences prudentielles distinctes d'annonce cyber pour les établissements couverts [S8].
- **FADP :** loi fédérale sur la protection des données (LPD), dont les obligations de violation dépendent des conditions légales [S7].
- **ISA :** loi sur la sécurité de l'information, fondant l'obligation d'annonce des infrastructures critiques décrite ici [S6].
- **CySA :** projet de loi sur la cybersécurité décrit dans la décision de rédaction 2026 du Conseil fédéral ; il n'est pas considéré comme adopté [S11].
- **MFA :** authentification multifacteur, exigeant plusieurs types de preuves pour se connecter.
- **Authentification résistante au phishing :** authentification liée au service prévu, réduisant l'utilité d'une fausse page de connexion.
- **DDoS :** déni de service distribué, trafic destiné à empêcher l'accès légitime à un service.
- **DMARC :** politique d'authentification des courriels aidant les destinataires à traiter les messages échouant aux vérifications d'alignement.
- **SPF / DKIM :** mécanismes d'authentification concernant l'envoi autorisé et la signature cryptographique du message.
- **DNSSEC :** signatures aidant les résolveurs validateurs à vérifier l'authenticité des informations DNS.
- **TLS :** chiffrement du transport utilisé notamment par HTTPS ; vérifier un certificat n'audite pas l'application.
- **HSTS :** politique web demandant aux navigateurs compatibles d'utiliser HTTPS pour l'hôte spécifié.
- **Enregistrement d'identifiants :** élément enregistré lié à un compte, possiblement historique, sans prouver un mot de passe actuel utilisable.
- **Association d'appareil :** lien entre un enregistrement d'appareil et un service ; il ne prouve indépendamment ni propriété ni infection actuelle.
- **Offre d'accès initial :** annonce revendiquant un chemin vers l'environnement d'une organisation, nécessitant validation.
- **Stealer :** logiciel malveillant collectant notamment identifiants ou données de session sur un appareil.
- **Inscription de rançongiciel :** revendication publique d'extorsion associée à un groupe et une organisation.
- **Fiche de publication :** reproduction expurgée d'un document clandestin conservé, avec date et limites explicites.
- **Incident fournisseur :** incident touchant un prestataire dont les informations ou services peuvent soutenir une autre organisation.

- **Enregistrement et personne :** un enregistrement est une entrée ; une personne peut figurer dans plusieurs entrées.
- **TLP:CLEAR :** désignation autorisant la diffusion sans restriction, sous réserve des autres obligations applicables.

À propos du rapport

Préparé par Odin by Brandefense pour la série Brandefense Country Report. Le texte maître anglais et les éditions allemande et française partagent identifiants de sources et fiches, figures et résultats numériques. Les traductions affichent une mention d'IA ; l'anglais prévaut en cas de divergence.

Ce dossier source soutient les décisions de sécurité et la vérification éditoriale ultérieure. Il n'est ni recensement exhaustif des incidents suisses ni certification d'une organisation. Les recommandations décrivent des travaux possibles pour les défenseurs, sans affirmer leur réalisation ou leur absence chez une organisation nommée.

© 2026 Brandefense. Tous droits réservés.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO